CYBERSPACE DEPENDENCE IN
AIR FORCE FLYING SQUADRONS AND ITS EFFECT ON
MISSION ASSURANCE

GRADUATE RESEARCH PROJECT

David D. Perez, Major, USAF

AFIT/ICW/ENG/10-04

DEPARTMENT OF THE AIR FORCE

AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED

The views expressed in this report are those of the author and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the United States Government.

AFIT/ICW/ENG/10-04

CYBERSPACE DEPENDENCE IN AIR FORCE FLYING SQUADRONS AND ITS EFFECT ON MISSION ASSURANCE

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Electrical & Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Cyber Warfare

David D. Perez

Major, USAF

June 2010

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED

AFIT/ICW/ENG/10-04

CYBERSPACE DEPENDENCE IN AIR FORCE FLYING SQUADRONS AND ITS EFFECT ON MISSION ASSURANCE

David D. Perez
Major, USAF

Approved:

//signed// 9 June 2010
Robert F. Mills, PhD (Chairman) Date

//signed// 9 June 2010
Michael R. Gramaila, PhD (Member) Date

AFIT/ICW/ENG/10-04

Abstract

The purpose of this research is to analyze the effects of cyberspace dependence in Air Force flying squadrons. The use of information technology (IT) in the workplace continues to transform the way squadrons conduct operations. While IT enables processes and capabilities, it also adds complexity and vulnerabilities. Therefore, airmen are required to have a higher technical aptitude as well increased awareness of their roles and responsibilities as routine operators of IT systems. This research focuses on exploring these issues and solutions at the squadron level.

In order to mitigate dependence on cyberspace at the unit level, the Air Force must address three key issues – squadron culture, squadron organization, and barriers to communication among key actors. Culture in today's Air Force fails to stress the importance of computers and networks in daily operations. Current organization in Air Force units provides no central coordination authority for cyber related issues. These problems are just a couple of the reasons that many barriers exist which prevent effective communication between network administrators and end users. Based on an in depth analysis of these issues, this research provides a framework for cultural and organizational change.

Acknowledgements

First and foremost, I want to thank my wife for her support throughout my Air Force career, and especially during my time at AFIT. I must also thank my young son who, along with my wife, keeps me smiling every day!

I would like to thank my research advisor, Dr. Bob Mills, for allowing and encouraging me to conduct this research project based on my personal experience. Although I may not have stepped far out of my comfort zone, this project has been a discovery of new thoughts and ideas that was made possible through his constructive feedback and expert direction.

Table of Contents

List of Figures

Page

Cyberspace Dependence in Air Force Flying Squadrons and its Effect on Mission Assurance

I. Introduction

> *The most basic theme is that conflicts will increasingly depend on, and revolve around, information and communications – "cyber" matters – broadly defined to include the related technological, organizational, and ideational structures of a society. Indeed, information-age modes of conflict (and crime) will be largely about "knowledge" – about who knows what, when, where, and why, and about how secure a society, military, or other actor feels about its knowledge of itself and of its adversaries.* (Arquilla and Ronfeldt, 1997)

Flying squadrons in the Air Force depend greatly on the control of information in order to accomplish their mission. Information, which was once deemed only a means by which to inform commanders and merely an enabler of operations, has become central to how squadrons fly, fight, and win (Libicki, 2000). If the mission of a flying squadron can be fundamentally defined as the production of effective sorties, then it is only through the equally effective control of information that its mission is accomplished. Therefore, a flying squadron's mission effectiveness is a direct result of how well its people collect, process, and disseminate information. In today's Air Force, the control of information is largely done through cyberspace.

The daily lives of airmen have been forever changed by the integration of, and dependence on computers, computer networks, and cyberspace. This change brings with it an uncertainty about how operations should be conducted within the cyberspace domain. Technology has proven to be a force multiplier and every day the Air Force requires that airmen perform more of their daily workload on computers and networks. The use of technology does not come without a price however. The hardware and software in use today have inherent vulnerabilities and are coupled with an emerging hacker threat (state or non-state) that seeks out new ways to exploit even those hardened and well-patched systems. With such an increased dependence on technology, and a similarly urgent need to secure cyberspace, it is imperative that the Air Force closely analyze how its core fighting unit – the squadron – is managing the challenges that cyberspace brings to the fight.

1.1 Background

If the trend that exists today continues, Air Force squadrons will continue to grow more and more dependent on technology. This trend will require that airmen have a higher technical aptitude and an increased awareness of their responsibilities as "cyber wingmen." This paper addresses the question of whether the Air Force is adequately preparing its forces – with an emphasis at the squadron level – for future conflicts that will require an expanded used of interconnected networks for operational requirements. Just as important though is the ever-growing need to secure those networks.

This balance – between operational requirements and network security – is the theme of this paper. While much attention is given to these ideas at higher levels, the discussion is lacking at the squadron level. The Air Force must begin addressing this balancing act, as it relates to the squadrons that are executing the mission. Ultimately the mission will depend not only on the technology in use, but also on airmen who must be trained and equipped to perform their duties in cyberspace.

1.2 Motivation

It was once possible for a well-prepared squadron to go to battle with a handful of computers that supported mission planning, intelligence, personnel data tracking, etc. Although computers were useful in previous wars, they were not essential to mission accomplishment. As late as Desert Storm in 1991, F-15E aircrew documented their efforts in mission planning which included sitting on the floor of a hangar, sifting through technical orders (hard copies in those days), and developing attack plans with grease pencils and maps (Smallwood, 1998). Their most advanced weaponry consisted of Laser Guided Bombs (LGBs) which can hardly be considered archaic since they are still widely used today. Yet their planning efforts and weapons employment depended largely on local information and very little on computers or networks. Their ability to employ weapons was limited only by their imagination, so long as they were able to comply with the weapons release parameters developed in mission planning.

Fast forward to Operation ENDURING FREEDOM (OEF) in 2010 where an F-15E aircrew is unable to mission plan a sortie without the use of not just one, but several computer systems. Basic flight planning is conducted with certain software, weaponeering is produced through different software, arriving at acceptable parameters for weapons release of a Joint Direct Attack Munition (JDAM) is done through a synthesis of information that takes into account aircraft parameters, weapon capabilities, and target structure. Today, all of this is done with computer systems. Aircrew must then carry cryptographic keys on a portable memory device to the aircraft, and likewise the JDAM itself must be “squirted” with a corresponding set of cryptographic keys thus allowing for secure interface with the weapon. Also, the JDAM uses Global Positioning

System (GPS) information to align itself to a pre-known position in order to recognize its own position relative to the target prior to weapons release thus enabling guidance to the target. Employment of weapons then depends not only on the ability of the aircrew, but on a multitude of factors that include interconnected systems, cryptographic algorithms, and globally provided navigation information.

The motivation for this paper is built on this scenario. The evolution of a simple process such as weapons attack planning into organized chaos, and the subsequent effect on war fighters. While some war fighters might be happy to go back to the days of grease pencils and paper maps, the reality is technology that creeps into practices today will only continue to permeate more and more. Are today's airmen prepared to deal with dependence on cyberspace, and is anyone willing to acknowledge that squadrons are assuming greater risk?

1.3 Purpose

> *Apart from the obvious ability to put a precision weapon anywhere within an identified command center, the really new feature of [Command-and-Control] warfare is the modern military's dependence on keeping information systems going – a dependence whose importance, in some respects, even surpasses the importance of keeping individual commanders safe from harm.* (Libicki, 2003)

This paper is a practical exploration of the growing dependence on cyberspace within Air Force flying squadrons and the subsequent side-effects that cyberspace dependence has on mission assurance. This project will analyze the transformation of certain practices, through the integration of cyberspace, which have changed the way squadrons conduct operations. Additionally, this paper will address the traditional construct of Air Force flying squadrons, and explore the need for change in the traditional responsibilities and components within a squadron.

In particular this paper is defined by the research question: *What impact has the Air Force's increased dependence on cyberspace had on flying squadrons?* In presenting answers to this general question, the research is further guided by the subsequent question: *How should Air Force squadrons adapt their structure and operations to better handle the challenges that cyberspace presents?*

The modest goal of this paper is to highlight issues that cause flying squadrons to struggle in the completion of their mission. It is not the intent of this paper to resort to "finger pointing" that places blame for these problems elsewhere. Instead, the intent is to shed light on the ways in which the Air Force can better organize, train, and equip airmen on cyberspace operations so that they can have a positive impact on mission assurance in their squadrons.

1.4 Scope

In developing the ideas and topics for this paper, the author relied heavily on over ten years of experience in operational flying squadrons, specifically fighter squadrons. The author therefore places commensurate emphasis on units that make up the flying community. However, it is clear that the problems addressed in this project do not constitute problems that are unique to the fighter community, or even the Air Force flying community in general. Since most, if not all, Air Force units are organized with the same general principles – institutionalism, vertical hierarchy, compulsory functional areas – the issues and propositions in this paper can then be logically inferred to all Air Force units that are faced with similar challenges.

In conducting an extensive literature review, common themes emerged that suggest the problems presented in this paper are neither unique nor unsolvable. The central themes are that of organizational and cultural change and provide the basis for much of the discussion in this paper. While change is discussed with regards to the flying squadron environment, it is done so with full consideration that the problems reach beyond the flying community and even the Air Force.

1.5 Organization

The research is divided into three parts that are dependent on one another and build upon the solutions presented for the research problem. The first part is presented in Chapter II and is a discussion centered on organizational and cultural change in the Air Force and how it is difficult when initiated from higher echelons. Much attention has been generated by senior leaders regarding the importance of securing cyberspace. While airmen read directives, mission and vision statements, and official memorandums from senior leaders, the leadership at the unit level is ultimately responsible for change within the unit. Therefore, organizational and cultural change should have a bottom-up approach. This approach provides the basis for why this paper focuses on change at the unit level.

Chapter III then addresses the first research question – the effect of cyberspace dependence on flying squadrons. This chapter analyzes the communication among the actors involved in the operation and security of network resources at the unit level. It is necessary to view this problem from the viewpoint of both network administrators and end users. This problem can be characterized as a barrier to communication that continues to grow as network security becomes more complex and stringent while end users are required to use technology more in their daily operations. This chapter addresses the need to bridge the gap between network administrators and end users.

Chapter IV ties the paper together with the third part of the research which deals with how flying squadrons can adapt their practices to better handle dependence on cyberspace. The emphasis here is that at the flying squadron level, there is a lack of advocacy and leadership to oversee and integrate cyberspace into operations. The chapter begins by introducing historical examples that presented the same types of problems that flying squadrons face today. Force Protection and Safety programs provide important case studies that had many associated unknowns and were ultimately solved through radical organizational and cultural change. These programs represent learning models which have strikingly similar characteristics to the challenges of cyberspace. Therefore, it is proposed that flying squadrons create and model their Cyber program after existing Force Protection and Safety programs. This would create an advocacy means to fully realize the capabilities of cyberspace in daily operations by giving airmen vital interaction with network security professionals. This program is designed to provide the three basic, yet necessary features to the squadron – communication channels, organizational accountability, and standardization of practices.

1.6 Key Terms and Definitions

Defining of the term *cyberspace* tends to stir up controversy since a wide variety of viewpoints exist that include different ideas and characteristics. Joint Publication 3-0 defines cyberspace as, "the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (2010). The scope of this research is limited to the Air Force squadron operating environment of computers and networks. Thus, for the purposes of this paper, the term *cyberspace* will refer to the "key components that constitute the domain, primarily *computers* and *networks* that interconnect them" (Courville, 2007).

The term *network administrator* will be used throughout this paper, and is intended to represent those war fighters who are struggling to secure networks. Since the research focuses primarily on cyberspace dependence and mission assurance at the squadron level, network administrators are typically represented by base communications personnel. Therefore, the term *base comm* will be used interchangeable with *network administrator*.

The terms *end users* and *operators* will be used interchangeably and represent those war fighters that use cyberspace to accomplish their respective mission. Again with the focus on the squadron level, *end users* or *operators* are assumed to be airmen serving in a typical flying squadron in the Air Force.

II. Organizational and Cultural Change

> *Today, we forge a long overdue Air Force cultural change. Cyber operations reinforce and enable everything we do – from administrative functions to combat operations – and we must treat our computers and networks similarly to our aircraft, satellites and missiles.* (Schwartz, 2009)

In May 2009, Air Force Chief of Staff General Norton Schwartz sent an e-mail to all airmen entitled *Cyberspace Operations Culture Change.* In this message, the Chief of Staff calls on all airmen to take action in the constantly evolving nature of cyberspace operations. This memorandum serves as the springboard for this chapter (and this overall project), to delve into the underlying culture issues that are the basis for the need to change attitudes and behavior among airmen.

The purpose of this chapter is to build a case for organizational and cultural change through squadron leadership. Units in today's Air Force are enveloped in cyber operations and although much dependence exists, the necessary emphasis on computers and networks, as more than just a means to an end, does not exist. In order to build a workforce that possesses both the capabilities to accomplish their duties through cyberspace operations and an awareness of the vulnerabilities and security challenges of cyberspace, the Air Force must address the culture that surrounds airmen at the unit level.

2.1 Air Force Culture Today

> *Organizational culture conveys a sense of identity for organization members, facilitates the generation of commitment to something larger than the self, enhances social system stability, and serves as a sense-making device that can guide and shape behavior. In turn, these factors can be used to build organizational commitment, convey a philosophy of management, legitimize activity and motivate personnel.* (Wiegmann and others, 2002)

It is unrealistic to think that one can offer a holistic view of modern military culture in a couple of paragraphs. Certainly the broad range of issues that shape the Air Force today are too many to list and therefore difficult to summarize here. Instead, the following simple illustration will serve as a snapshot of the ideals, behaviors, and attitudes that are likely to be found among airmen today.

In *Employee Warriors and the Future of the American Fighting Force*, Major Hugh Vest explores the conflict between the "traditional values and culture once associated with a successful fighting force," and the "elements of the business-scientific/management-professional culture" associated with the modern occupational military (2002). Vest hits the nail on the head when he asks, "Why does today's service member seem to identify more with the managerial lampoons of the comic strip *Dilbert* than with the traditional military humor in *Beetle Bailey*?" (2002) After all, today's military does not conjure up an image of a drill sergeant screaming at a young, quivering trainee. Instead, the image often associated with the modern military, certainly true for today's Air Force, is that of a war fighter monitoring information via multiple computer screens and responding to events with clicks of a mouse. This is not just indicative of a clerk conducting administrative actions in an office building, but is also true for soldiers conducting combat operations via video feeds from Unmanned Aerial Vehicles (UAV) to strike targets in OEF.

Indeed, today's Air Force alienates many of the paradigms of traditional military culture, and the movement to deeply embed practices and procedures in science and technology is culpable. Vest goes on to paint a picture of the cyber warrior of the twenty-first century, and offers that today's military is at a crossroads between gradually eroding traditional culture and the technology driven future (2002). Today's war fighters, shaped in the information age, are confronted with mixed signals from elements that dominated military culture in the past (institutionalism, hierarchy, fraternity) and current ideals (diversity, individualism, equality) (Vest, 2002).

> The continuing challenge for military planners is to place these new information technologies and capabilities into a logical construct with ties to current and past military thought and operations. (Harshberger and Ochmanek, 1999)

The conflict described by Vest manifests itself in the daily operations of flying units throughout the Air Force. If one were to walk into a flying squadron today, they would find airmen tucked away in offices and cubicles. These workspaces represent treasured real estate that was no doubt staked the day the airmen arrived at the unit, for without a "place to call home" at work, airmen feel worthless. No workstation is complete without a computer that ideally represents the latest in technology, lest airmen be relegated to conducting their business on an older, slower machine that meets their needs but not necessarily their wants. Communications, even official orders and requests, are done electronically – airmen do not even bother to swivel to speak with the person at the next workstation, instead they send an e-mail. What's more, in dealing with bureaucracy, airmen will ban together to throw jabs at "upper management." As Vest suggests, all this makes the atmosphere of a flying unit feel a lot more like *Dilbert* vice *Beetle Bailey* (2002).

One final note about culture in flying organizations is the critical notion that the same technology that empowers airmen in the workplace also serves to isolate airmen. "At the micro-level, technical specialization is leading to isolation within organizations, even for functions that should overlap. Soldiers within a given service, base, wing, platoon, or squadron find few common threads" (Vest, 2002). With an isolated workforce, the danger is that airmen will foster the attitude that "no one is watching." Unfortunately, this is the culture of the Air Force today – a culture of decreased accountability due to the isolation and individualism of airmen. If the Air Force is going to positively alter the culture of airmen at the unit level, it must address this attitude in particular. While many aspects of culture deserve attention, it is the lack of accountability caused by the sense of isolation that will be explored further in this chapter. However, before specifically addressing accountability, we must first address a roadmap for how the Air Force can best tackle this major issue. It is here that the notion of a bottom-up approach to culture change is introduced.

2.2 Bottom-Up Approach

The enormity of cyberspace operations in the workplace requires that airmen clearly understand their roles and responsibilities as operators of computer systems. While it is easy to find speeches from flag officers and articles written by scholars and students of doctrine that generalize the Air Force approach to cyberspace, it is very difficult to find *direction* from any of these sources.

> The Air Force has concluded that the cyberspace domain underpins every aspect of war fighting simultaneously at all levels of operations and that cyber capabilities are being rapidly developed as well as globally dispersed. However, its task of clearly and simply articulating what airmen do in cyberspace and how they do it as war fighters remains. (Convertino and others, 2007).

Clear direction is necessary in order to ensure that the presence of airmen in the cyberspace domain both enhances the combat capabilities of the Air Force and, more importantly, does not create a vulnerability to Air Force networks.

So who should articulate to airmen what they should do in cyberspace and how they should do it? If General Schwartz' message on culture change is taken at face value, one might think that direction is required from the highest echelons in the Air Force. At the strategic level, this is essentially correct, since the common goal is to defend the Air Force Global Information Grid (AF-GIG), which is a strategic war fighting tool. But for airmen spread out in various types of units throughout the Air Force and operating with a specific focus or task, it is not necessarily a strategic fight. Airmen contribute to the fight in a more localized, tactical setting. Subsequently, and not surprisingly, what airmen do is a direct result of their squadron leadership and direction. This perspective on leadership and direction, through the eyes of airmen on the front lines, suggests that culture change is best applied in a bottom-up approach.

> First, [policy] is often created by a top-down directive and the goal is to determine the best construct to achieve the already defined objective. Second, it is created from the bottom-up, reflecting a determination to ask the subject matter experts to develop their best response to a problem and propose a coherent solution. (National Security Threats in Cyberspace, 2009)

The idea that culture change in an organization can work bottom-up is counter intuitive. The Air Force generally tends to confront problems in a top-down or big-to-small approach. This traditional approach is a product of an institution that is organized vertically. Members look upward for broad tasks and direction, then parse out components to subordinates below. In the war fighting arena, this approach is analogous to the process of selecting which targets to bomb. Generally, the first step is to analyze the centers of gravity, then numerous processes are carried out to nominate and prioritize targets, with the final result being a comprehensive list of targets that represent the tactical solution to the strategic problem.

But in the case of rapidly evolving computer systems, applying a top-down approach is a challenge. While broad direction that prioritizes the security of cyberspace can define the strategic problem, how that translates down to each individual unit will differ dramatically. This makes it difficult to identify a comprehensive tactical solution that encompasses all squadrons for a variety of reasons.

First, not all Air Force squadrons are created equal when it comes to cyberspace. Different organizations have their own unique characteristics, missions, priorities, and operating environments. Although the Air Force attempts to standardize cyberspace capabilities, there will inevitably be differences among organizations. Air Force leadership cannot be expected to know each and every computer system that equips airmen. Therefore, it makes it very difficult for higher echelons to develop specific policies that apply to every unit.

Second, as the Air Force continues to develop a mindset towards cyber warfare it is easy to think that this type of warfare will always be global in nature. Efforts to centralize networks (discussed in Chapter III) suggest that the Air Force is better equipped to fight a cyber war with central control over its global resources. The uncertainty of this aspect of cyber warfare is beyond the scope of this paper; however, it is important to note that localized attacks are a likely vector for adversaries to exploit, making it important to have cyberspace awareness at the unit level. Indeed, it may be an airman operating in his or her unit that raises the initial flag that the network is being attacked. That is, if airmen are properly equipped to do so, with training and oversight that teaches them to identify and report nuances in the network.

Third, computer end systems that are used at the squadron level represent the "front lines" of the cyberspace battlefield for the Air Force. "Every soldier, airman, and marine is on the front line of cyber warfare every day" (Chilton, 2009). While it may be a stretch to call every airman a "cyber warrior," the role of security in cyberspace lies firmly with every airman who logs in to a computer on his or her desk. Is it reasonable to expect that broad, strategic level emphasis on security will eventually filter down to that airman?

"Securing our systems must come from a bottom-up process and not be delayed while we wait for a top-down initiative" (Janczewski and Colarik, 2005). The Air Force can no longer wait for top down initiatives to filter down to airmen and must institute actions that directly impact the cyberspace awareness of airmen at the unit level. The Air Force stands to make great gains by better equipping the airmen on the "front lines of cyberspace."

At this point the author will indulge a bit in offering further support to the idea of a bottom-up approach. Consider aircraft struggling for superiority in the air domain. When conducting offensive and defensive counter air missions, the entire Air Force does not attack en masse with only broad direction from General Officers. Instead the problem is broken down into smaller tactical portions. These tactical problems are then tasked to smaller elements (4-ships or 2-ships) to solve. The really big problem is broken down into smaller, manageable pieces and the result is executed with central control and focus. This ensures the big problem is solved while maintaining sufficient oversight over the individual elements in each fight. Essentially, the basic concept described here is centralized control and decentralized execution. While broad direction is given in the form of central control, the tactical portion is executed at the micro-level. Should the Air Force use the same strategy when confronting cyberspace culture change? Perhaps the Air Force should simply provide broad direction that enables the problem to be broken down into manageable pieces – i.e. tasking and holding accountable individual organizations (i.e., squadrons) to operate and regulate their own use of computers and networks while maintaining sufficient awareness and control at the broader level.

The bottom-up approach will only work however, if sufficiently high priority is placed on this effort by squadron leadership. Therefore, it is important that squadrons have a roadmap, developed and supported by unit leadership, to effectively institute culture change using the bottom-up approach.

2.3 Squadron Leadership and Cyberspace

> *But whatever [cyberspace] organizational structure we choose in the end, the fundamental question will come down to one of leadership.* (National Security Threats in Cyberspace, 2009)

For squadron commanders, the sheer size and scope of cyberspace can be intimidating, particularly to those commanders who do not possess technical degrees or expertise in information technology (IT). This in turn can contribute to a lack of confidence when dealing with cyberspace issues. Instead of viewing computer networks as a war fighting tool, squadron commanders depend on resident computer expertise to provide “just enough” information while avoiding intricate details. To make matters worse, computer expertise within squadrons has been "complicated by shrinking manpower and funding" in recent years (Fulghum, 2009). That means fewer Client Support Administrators (CSA) for commanders to rely on to do workgroup management and daily housekeeping of their networks. Although squadrons do not own the administrative rights of the computers and networks in their units, commanders should have sufficient on-hand expertise to assist in decision-making, assessments, and oversight of the end systems that they do own.

Every squadron commander is responsible for computers that represent end systems on the greater AF-GIG. And commanders are also responsible for the people that operate on those end systems to accomplish the mission. Every time a computer is added to the AF-GIG, it is incumbent that someone takes responsibility for that computer, its connection to the network, content, and usage within regulation and protocol. Likewise, every user that is certified to operate a computer on the AF-GIG should be held accountable for their operations on the network. Squadron commanders can no longer stiff arm this responsibility. This is where leadership in cyberspace begins – by taking accountability for computers and networks and the war fighters that use them.

2.4 Culture of Accountability

> *Success springs from the willingness of an organization's people to embrace accountability.* (Connors and others, 1994).

In order to change Air Force culture with regards to cyber operations, leaders must address the issue of accountability within their organizations. It is important to understand that this type of fundamental change begins with individuals. "Even though the *initial focus* of an organizational change may be to change some aspect of technology, or of the organization's tasks and structure, the ultimate impact will be on people" (Albanese, 1975).

There is an important distinction to make when discussing organizational accountability that requires attention be given to two specific aspects. First, squadron commanders have the right and responsibility to hold their people to a high standard of accountability. Whether it is an extreme case that calls for a commander to punish an airman under the Uniformed Code of Military Justice (UCMJ), or a smaller offense that perhaps violated only a local squadron policy, ultimately the squadron commander can hold airmen accountable for their actions. That is the first aspect and certainly an important one. The second aspect that requires just as much attention is the notion that one can gauge the accountability of airmen by their level of ownership and participation. These two distinctions – holding airmen accountable for their actions *and* fostering a culture of ownership and participation – represent separate challenges for Air Force squadron commanders.

2.5 Accountability for Actions

Culture change begins with Air Force leaders holding their people accountable for their actions in cyberspace. Of course this is easier said than done. Airmen are doing more on computer systems now than ever before and it is difficult to predict, from one day to the next, what new software tool, e-mail policy, or sophisticated gadget will enter their workplace. This does not change the fact that squadron commanders must be involved in their unit's daily cyber activities.

To what extent can a squadron commander really be involved in cyber activities of his or her people? Of course it is impossible to monitor every e-mail, word document, or mission planning product. Nonetheless, it is still possible to be involved. It starts with clear policies, rules, and regulations. Do these already exist? Of course, every airman has to complete online Information Assurance and Information Protection training annually. Annual online training is a broad stroke solution that has had *very* limited success in improving the conduct of airmen in cyberspace.

> I am required to train on cyberspace security once a year ... Once a year! During the training, I get to read and study year-old tactics, techniques, and procedures used by an adversary who is modifying them every day, perhaps every hour. We are not training appropriately, and we need to change that. (Chilton, 2009)

This annual training is not enough, and more direct contact with airmen that addresses specific conduct issues is necessary in order to truly have an impact on accountability.

2.6 Develop Squadron Policy

In their book *Managerial Guide for Handling Cyber-Terrorism and Information Warfare,* Lech Janczewski and Andrew Colarik advocate the need for organizations at the lowest level to implement and enforce strict information security policies. Figure 1 lists the specific areas that Janczewski and Colarik recommend information security policies address.

- System Planning and Acceptance
- Protection Against Malicious Software
- Housekeeping
- Network Management
- Media Handling and Storage
- Exchange of Information and Software
- System Development and Maintenance
- Compliance

Figure 1. Information Security Policy (Janczewski and Colarik, 2005)

Air Force squadrons create and maintain various forms of standard operating procedures (SOPs). However, it is safe to presume that most units do not include any form of strict policy that outlines their computer operations to supplement existing Air Force Information Assurance (IA) policy. Well-developed SOPs allow the squadron commander to convey to his or her airmen precisely what is expected of them with regards to their roles and responsibilities in cyberspace. Squadron commanders must develop and implement policy that, at a minimum, addresses the issues in Figure 1. This affords the squadron commander the ability to tailor policy to the specific needs of the unit and the ability to enforce and regulate the actions of his or her airmen. And they serve as protection measures against network attacks and malicious actions since many of the issues not only address efficiency but also security and safety in cyberspace (Janczewski and Colarik, 2005).

2.7 Enforce Policy

Many assumptions can be made regarding the daily activities of a squadron – that all airmen will participate within the rules, that all airmen arrive at work with the willingness to contribute to the fight and make their unit better, and that airmen have good intentions for their actions. While these assumptions are true most of the time, obviously some airmen get into trouble, disobey lawful orders, or behave with less than good intentions. When cyberspace operations are involved, lines that were already gray can be muddied even further. It is imperative that squadron commanders enforce their cyberspace SOPs. When violations of SOPs occur, commanders should stand ready to hand out the appropriate punishment. Violations can be divided into three categories that warrant further discussion: mistakes, work-arounds, and malicious actions.

Mistakes happen all the time, to hard working people who comply with policy and have good intentions. Mistakes can range from situations where someone fails to log off and leaves their CAC in their computer unattended, introduces a virus onto the network from what they believed to be a trusted source of media, or inadvertently damages computer equipment. A well-developed squadron policy will include varying levels of repercussions for mistakes. These should have two characteristics. First, punishment should be at the discretion of the squadron commander – for only he or she can best be the judge of the severity of the mistake and the intent of the person who committed the error. Second, the punishment should fit the crime. For minor infractions – i.e. use of non-approved hardware or software on the Nonsecure Internet Protocol Router Network (NIPRNET) – a simple action such as verbal counseling might suffice. For more serious offenses – i.e. unintentionally infecting multiple systems with malicious code through the use of a non-approved memory device – the commander should have the ability, and not hesitate, to revoke network privileges until the individual is retrained and recertified.

Next is the issue of work-arounds. If a random airman was interviewed on their daily practices in the workplace, he or she will be able to quickly point out the procedures, rules, and processes that are holding him or her back. Even worse, it is nearly impossible to justify these procedures, rules and processes once they are deemed an obstacle (Horton, 1992). Unfortunately, a part of daily life in any given squadron is that work-arounds exist and in many cases airmen have come to depend on them. Work-arounds are actions taken which subvert safety and/or security in order to get the job done. Bypassing security in this way is dangerous since it can introduce vulnerabilities onto the network. It is also dangerous since it sets the precedent that SOPs and/or IA policies are not important. If a young Lieutenant sees a Field Grade Officer (FGO) transfer data from a classified system to an unclassified system, what kind of message does that send?

For the squadron commander, this issue can be broken down into three simple questions. Why was the work-around initiated? Was the work-around really the *only* option? What action (if any) can be taken to remedy the condition that caused individuals to seek an alternative action? Of course there may be other questions to ask, but from the perspective of a leader in cyberspace, the goal should be to identify those obstacles that keep airmen from executing their duties and attempt to remedy those obstacles. If a remedy is not available, then the commander should take action that reiterates the importance of IA policy and unit SOPs, as well as the mission of the squadron.

It is important to note that work-arounds can, and sometimes are, initiated for legitimate reasons. A classic example of a legitimate work-around is the transfer of "mission essential" data from one computer system to another. This issue stems from the fact that, strangely enough, memory devices work exactly the same on NIPRNET and SIPRNET computers. Therefore, inevitably there comes a time when an airmen has data (perhaps a squadron flying schedule) that must be transferred between the NIPRNET and the SIPRNET. With no other option available, airmen are forced to use portable media for this type of data transfer. Although this work-around can be characterized as legitimate, it does not make it any less of a threat to network security. Therefore, commanders should immediately take action to incorporate improved procedures or processes that allow "mission essential" information to be shared without threatening network security. It is only when all available options have been exhausted that commanders should allow a work-around such as this to continue.

Finally, there is the case of malicious actions. Computers and networks are used every day be people with malicious intent. Commanders cannot assume that people in the Air Force would never commit malicious acts within military networks. It goes without saying that commanders should pursue swift and severe punishment for those involved in malicious computer actions. However, just because these acts can be initiated from within Air Force networks does not make it any easier to identify the source or individual. Just as the "Eagle Eyes" program does for Force Protection, so too should airmen be on the look-out for suspicious or deviant behavior among network users. The culture of ownership and participation is a key principle in rooting out deviant behavior within organizations in the Air Force.

2.8 Accountability through Ownership and Participation

> *It is in our own best interest in such changing times to direct our future operating environment through active participation. Communication networks only can be protected against attacks if all stakeholders participate.* (Janczewski and Colarik, 2005)

When the average airman arrives at work, he or she will use a computer to complete some or all of their tasks. Some airmen, undoubtedly, take the computer they use for granted. They will turn it on, log in, get what they need, and move on. Very few airmen will take the time to ensure the computer is clean, operating correctly, and secured properly. "We must treat our computers and networks similarly to our aircraft, satellites and missiles" (Schwartz, 2009). Ownership is a key concept in creating an atmosphere of accountability in cyber operations.

2.9 "It's not my job"

When something is not working properly, too often airmen will just walk away. It is easy to do when there is another computer at the next desk that is vacant. Take for instance a printer that has malfunctioned and an individual who has exhausted his or her knowledge of possible fixes. The first thing the individual does, instead of contacting the appropriate administrator, will be to seek an alternative printer that is working so they can get their work done. Situations such as these cause computer equipment to sit broken, without repair for days, weeks, or even years. The problem is not that no one knows how to fix the equipment – the problem is the right people are not informed about the broken equipment in the first place. So airmen sit next to broken equipment "waiting to see if some hoped-for miracle will be bestowed by an imaginary wizard" (Connors and others, 1994).

2.10 Own it

How would a culture of accountability change the above scenario? Once again, this relates back to the squadron culture and the policies developed by commanders. It starts with emphasis on equipment. Although every Air Force unit must maintain an inventory of their computer equipment, IT systems have been known to go missing without any explanation. Follow-on investigations usually result in finger-pointing, denial, and excuses. The culture of cyber accountability does not exist in these units.

If a production superintendent in an F-15 Aircraft Maintenance Unit (AMU) was asked about a specific jet on the flight line, he or she would be able to provide the current condition of the jet – flyable or not flyable. If a jet is not flyable, there would be information about why the jet is broken, where the parts are in the supply chain, and when the jet is expected to be fixed. The Air Force has set precedence for being able to track such minute details. Why do computers and computer networks receive so much neglect?

The policies developed at the unit level should strictly enforce housekeeping and inventory procedures for computer equipment. Of course, the Automatic Data Processing Equipment (ADPE) program exists to manage and account for computer equipment. However, this is often an additional duty and does not receive sufficient attention – that is until equipment goes missing. Through housekeeping practices – routine maintenance, updating, cleaning – leadership sends a message to airmen that the equipment is important. And with good inventory procedures, squadron leadership is better able to accurately identify the status of the unit's equipment, network, and cyberspace capabilities.

A squadron that has developed and implemented policies to sufficiently manage their own cyberspace resources is then better able to handle relationships with the agencies and individuals that administer those resources. So it is logical next to explore the relationship between personnel at the squadron level and network administrators.

III. Barriers Between Network Administrators and End Users

> *The dependence on cyberspace of US weapon systems, critical infrastructure, financial institutions, and our way of life creates an imperative to operate freely in this domain.* (Jabbour, 2009)

As cyber operations continue to expand in units throughout the Air Force, network security and mission assurance have a tendency to be at opposite ends of the spectrum. At the unit level, where the mission is paramount, this creates the possibility of collisions between concerns over network security and requirements for mission accomplishment. What is often forgotten is that throughout the Air Force, the mission relies on a myriad of systems and capabilities. Efforts to secure cyberspace, can have unintended consequences on those systems and capabilities, that in turn can have unintended consequences on the mission. The Air Force must realize that the mission is not immune to disruption, and certainly efforts to secure cyberspace can disrupt the mission.

The purpose of the chapter is to reveal how the effects of network security are felt at the unit level, by both end users and the mission. To do so, it is necessary to explore the fragile relationship between network administrators and end users. With an understanding of the underlying issues that strain this relationship, an analysis of the cost of network security will lay an additional framework for this unique problem.

3.1 Background

> *The lack of a comprehensive defense against the increasing cyberspace threat over the past twenty years provides the backdrop for the Air Force and its vulnerable computer systems and domain it has today.* (Courville, 2007)

In *Air Force and the Cyberspace Mission, Defending the Air Force's Computer Network in the Future*, Lt Col Shane P. Courville's critical analysis of the evolution of cyberspace dependence reveals some interesting characteristics about Air Force networks. He describes how the Air Force's initial curiosity in cyberspace began in the 1980s and 1990s when the Air Force began slowly expanding its use of computers. During this period, Courville explains, airmen who did the majority of their *typing* on a *typewriter* witnessed the introduction of the desktop computer to the workplace (2007). At first it was a single workstation that was used in a central location by a group of users, but rapidly advanced to the point where every individual in the Air Force had a computer available to them.

Courville notes that this initial transition period is the basis for many of the struggles with network security today (2007). The acquisition and implementation of computer systems was relegated to the wing level. This made sense since wing level personnel would best be able to acquire those machines that met their mission specific needs. The technology purchased at the wing level during this time would serve as the end systems with which the Air Force, along with all of America, began to embrace the interconnectivity of networks. Although initially a far cry from a centrally "controlled" network, this architecture provides the basis for today's NIPRNET.

The computers that make up the NIPRNET, and therefore the AF-GIG, have been assembled over time without the principal concern of security. So the internet and, consequently, the NIPRNET are constructed similarly to a trailer park, where anyone can arrive and plug in with whatever equipment they bring with them. In *Cyber Security: A*

Crisis of Prioritization, published by the President's Information Technology Advisory Committee, it is noted that:

> The Internet – now a global network of networks linking more than 300 million computers worldwide – was designed in the spirit of trust. Neither the protocols for network communication nor the software governing computing systems (nodes) connected to the network were architected to operate in an environment in which they are under attack. (2005)

This ad hoc nature of interconnectivity introduces vulnerabilities that the Air Force must deal with at a broad level. Because there was uncertainty about which systems would work best, and freedom was given to Air Force wings to buy and implement whatever they chose with minimal overarching guidance. The Air Force has spent the past ten years trying to consolidate and standardize equipment to overcome the initial impromptu procurement of end systems. Nonetheless, the resulting network is still difficult to define and defend.

With this baseline knowledge on the evolution of Air Force networks, it is now time to give attention to the people charged with defending these networks. While the bulk of this chapter will focus on network administrators that control networks from central locations, it is first necessary to study the roles and responsibilities of squadron CSAs. Upon taking a closer look at the role of CSAs, it is interesting that although they are meant to be a means to bridge the communication gap, the CSA career field is vastly underutilized.

3.2 Current Organization

The CSA career field, like many others, has experienced a significant decline in personnel due to recent force shaping initiatives in the Air Force. While the career field is made up of professional, hard-working airmen, three key factors hinder their ability to remain actively engaged in the integration of cyberspace operations. First, the evolution of CSA roles and responsibilities has caused significant role conflict and role ambiguity (Johnson, 2003). Second, CSAs have been stripped of network administrator privileges which severely limits their ability to manage cyberspace related issues. Third, CSAs do not possess appropriate rank and experience to effectively serve as a liaison or advocate for the units they represent.

The roles and responsibilities of CSAs have undergone a significant transformation. Once rooted in the traditional role of Information Management (IM), today's CSA workforce is responsible for "multidimensional, general tasks that involve the entire process of managing information" (Johnson, 2003). The advent of technology in the workplace has forced the CSA career field to accept greater responsibility in the "front-line support for the life-cycle management of information" (Johnson, 2003). In other words, CSAs are not only responsible for overseeing the management of information, but they also oversee the systems used to manage the information – namely computers and networks. Given their direct contact with squadron computer resources, ideally, CSAs would be the central liaison between the unit and the higher echelons of computer and network control. That is, if these roles truly represented what CSAs *actually* do.

Since squadron orderly rooms have been consolidated at the group and sometimes wing level, this has forced squadron commanders to come up with creative ways to man their commander's support staff (CSS). So, the more likely scenario is that CSAs are "assigned to personnel billets within unit orderly rooms and expected to perform personnel-related work (e.g., manage personnel actions)" (Johnson, 2003). Unit CSAs are essentially used as an ad hoc CSS meaning they do more personnel management and less IT support. Furthermore, CSAs today are assigned a myriad of additional duties such as resource advisor, building custodian, etc. Their job descriptions read more like a laundry list of additional duties than IT or network administration related functions. Also, the roles of a CSA in one unit will be vastly different than the roles of a CSA in another unit, causing a lack of standardization across the career field. It is easy to see why many CSAs feel a tremendous sense of role conflict and role ambiguity since their duties are not clearly defined (Johnson, 2003). The incentive for squadron commanders to employ CSAs as "personnelists," thereby negating their IT expertise, is due partly to the diminished role that CSAs have in administering the network.

Today's CSA workforce at the unit level does not have administrator privileges on computer systems as in the past. This is a side-effect of the centralization of networks which will be discussed in detail later. More and more, administration and control is moving to higher echelons which means that CSAs responding to customer needs within their unit can do nothing more than make a phone call to the *actual* network administrator. CSAs are effectively now just first responders with an extremely limited toolkit. Simple desktop maintenance, software patching, and password resets are not even possible at the unit level rendering the CSA workforce helpless when attempting to address computer related issues in their units.

Adding to this problem is the notion that managing the network at the unit level requires appropriate rank and experience to deal with the respective customer of different organizations. Since this research is focused on change among flying organizations, it is a fair statement that a Senior Airman dealing with a flying unit of 60-70 officers will have a much more challenging time making necessary changes to squadron culture (accountability, participation, ownership, etc.). Is it fair to put an Airman or even a junior NCO is the awkward position of confronting officers about their daily procedures and practices?

Having examined the characteristics of unit CSAs, the discussion now turns to network security from the administrator's perspective. Keeping in mind the limited ability of the CSA work force to bridge the communication gap, the next section will introduce the multitude of barriers to communication that exist among key actors at the unit level.

3.3 Security – Network Administrator's Perspective

> *Every new or improved capability, however, no matter how dominant, brings with it a whole new set of inherent vulnerabilities*. (Lovelace, 2005)

Clearly, the security of Air Force networks represents a difficult challenge. In discussing the specific reasons that exasperate the administrator's efforts to secure networks, this section will begin to paint the picture of the fragile relationship between network administrators and end users. The end user, in eyes of the network administrator, can be the greatest threat to network security. A variety of issues contribute to this mentality, ranging from individual actions of end users to the previously discussed nature of Air Force networks which makes them difficult to define and defend.

First, network security is complicated when commanders, who are themselves end users, want to add more capability to their unit and simply add more nodes to the network. This makes the network difficult to define. “When I asked last year how many [SIPRNET and NIPRNET] machines were on the DoD network, it took more than 45 days to get the answer – and I’m not sure I got the right answer” (Chilton, 2009). While there are governing rules that oversee the expansion of the network, it is increasingly difficult for administrators to maintain situational awareness since the network is in a constant state of evolution.

> Changes in the cyber domain occur with great rapidity, based on ever advancing computational and communications technology. The interconnectedness of cyberspace enhances this consequence of acceleration. Vexingly, each change creates a new cycle of vulnerability and response. Far from being static, cyberspace is almost overwhelmingly dynamic. (National Security Threats in Cyberspace, 2009)

Furthermore, Courville offers that “the lack of standardization Air Force-wide during implementation of the domain over the past decades” causes headaches for network administrators who must leverage compliance between legacy systems that end users in the Air Force rely on and the expansion and advancement of systems to meet emerging needs (2007). “There are too few security safeguards to protect the cyber environment especially with the exponential growth of both capability and associated risk as the Air Force’s domain continues to grow” (Courville, 2007).

Second, the network is difficult to defend because network security depends greatly on each and every stakeholder. In essence, network administrators need “buy-in” from every end user who operates on the network – and that is difficult to achieve. The fundamental paradox of security is that network administrators constantly strive to provide access to those who need it, but must simultaneously safeguard information from those who seek it, yet have no need or right to access. So network administrators spend countless hours on this balancing act. All of their efforts mean nothing if just one user chooses to step out of line and violate policy, and in turn introduces a vulnerability to the network, knowingly or unknowingly. “The greatest current problem, however, is and is likely to remain human factors” (National Security Threats in Cyberspace, 2009).

There is much documentation which identifies the end user as the weakest link in security (Schneier, 2000; Leidigh, 2005; Miller and Gregg, 2006). The earlier discussion of mistakes, work-arounds, and malicious actions are examples of ways in which airmen, operating as end users, are tempted or forced to do things that are bad for network security. Users simply cannot or will not remain within the boundaries of a well-developed acceptable use policy. User error, whether unintentional or malevolent, further weakens the network since vital time and resources are used fixing rather than improving the network. “Today, the amount of time spent repairing a network due to just a single worm or virus attack can easily be greater than the upfront time to more adequately secure an enterprise” (Leidigh, 2005).

Third, network security is made difficult by attackers themselves who modify their attack vectors daily, if not hourly, and continually target the end user. While administrators play “zone defense” to find attack vectors and plug holes in the wall of defense, they do so knowing that one end user can severely cripple the network with just one click – for example, by simply opening an e-mail attachment that is part of a spear-phishing attack. Administrators then have to balance their efforts to secure the “buy-in” discussed above while simultaneously reacting to the emerging hacker threat. Knowing that not all users will behave, security is then reactive to the current threat which will be different tomorrow and the next day

> Today, as in the past, DoD remains in a constant *reactionary* mode to secure itself from cyberspace infiltration. After over two decades of experience in the cyber domain, DoD's improvements have been minimal and there are serious issues that continue to plague DoD when trying to protect its computer systems. (Courville, 2007)

Fourth, the advancement of technology in the workplace has led to a culture where airmen are evaluated on innovation. Because technology is flexible in what it can provide, airmen have learned that they can make great strides by manipulating processes and practices to improve operations. The evidence exists in any Officer Performance Report (OPR) or Enlisted Performance Report (EPR), where one is sure to find accolades proclaiming the individual's contribution to the mission by developing new capability X or improving operations by X%. "In a tight resource environment, these practices manifest themselves in the *do more with less* syndrome" (Vest, 2002).

The clash between network administrators and end users is fueled by these factors making the limited opportunities for communication between these entities scarce. Another contributing factor that one would do well to explore is the effects of the movement to centralized control of Air Force networks.

3.4 Centralized Control

Efforts in recent years to centralize the control of the AF-GIG are one measure by which the Air Force hopes to improve network security. The centralization of network control is an attractive option since it offers many features that will ease the burden of network security. However, as this section will discuss, the advantage of centralizing the AF-GIG does not come without some costs that produce additional barriers between administrators and end users.

In *Who Runs What in the Global Information Grid*, Libicki offers a comparison of the cases for both centralization and decentralization (2000). On centralization he notes:

> Difficult problems of coordination, coupled with the potentially overlapping responsibilities in any complex endeavor, often raise demands that someone be placed in charge of an enterprise so that power is concentrated in those who then bear the onus of making something work (rather than spread among those who can conveniently point to someone else when it does not).

Libicki goes on to point out that centralized networks are able to fill global management gaps. This alleviates every unit determining for itself how to properly operate and defend their own network. Centralization also enables the synchronization and synthesis of information, which in turn facilitates coherent and coordinated information exchanges among actors globally. Ultimately the vision is that of a Common Operating Picture (COP), which efficiently concentrated resources can provide, for better network defense, threat detection, etc. In essence, this "puts someone in charge" of information exchange and for network security this can be a great advantage.

What is good for the defense of the network has some side-effects though. First, the cyber domain, as discussed earlier, does not necessarily lend itself nicely to the centralized concept.

> Paradoxically, despite the concentration of specialized knowledge required, the distributed nature of the cyber domain prevents any one single person or group from exercising complete control. Because of the interconnectedness and interoperability of cyberspace, no locus of positive control if feasible. (National Security Threats in Cyberspace, 2009)

Despite the conceptual advantages, a centralized network is difficult to *control*, particularly in a dynamic environment, such as that of the Air Force today.

Furthermore, the centralization of networks tends to hinder the ability of users to coordinate information among themselves (Libicki, 2000). It turns out that synthesis of information is difficult to achieve through central control. Information is supposed to fit the requirements of its users, who would like to have flexibility to make decisions on their own. Libicki points that in the centrally controlled network, users do not necessarily get what they need, rather the product that trickles down is merely a "guess at what users need" (2000).

Centralization is a key to network security. By moving towards a COP, concentrating resources, and identifying requirements at the global level, the Air Force is making strides in network security. However, the discussion above clearly shows that already limited communication channels between network administrators and end users are only further strained through centralization.

3.5 Barriers to Communication

Thus far, this research has introduced organizational and cultural issues that shape the cyberspace operating environment in Air Force flying squadrons. Also, the previous discussion characterized the wide variety of issues that administrators deal with in their struggle to secure the networks. Seen together, these concepts paint a picture of the increasingly strained relationship between network administrators (i.e. base comm) and end users (squadron personnel).

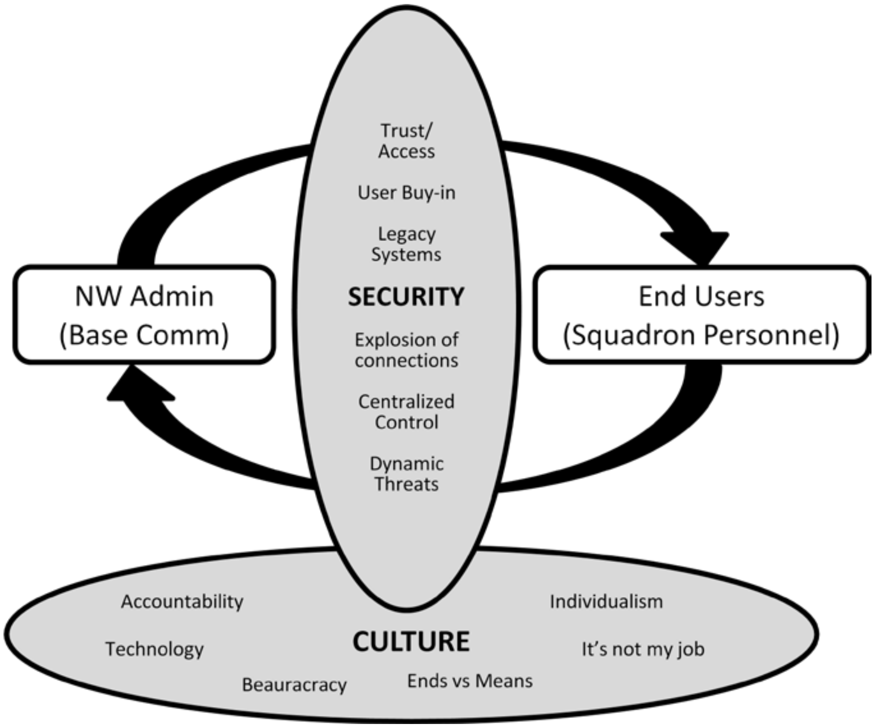


Figure 2. Barriers to Communication

Having looked at the administrator's perspective, it is likewise necessary to view this relationship from the viewpoint of the end user.

3.6 Security – End User's Perspective

> *Security costs money, hassles users, often denies service to the legitimate, and is prone to failure if users react by subverting its rules.* (Libicki, 2003)

If the end user is seen as a threat to network security in the eyes of the administrator, then it is only fair to address the inverse relationship as well. Since at the unit level the mission is paramount, then how is network security characterized? A likewise general statement that the network administrator is, in the eyes of the end user, an "obstacle to mission success" should be similarly explored.

Consider network security from the perspective of an average airman in a random location in the Air Force. The question is – how important is network security to that airman? With all the discussion about airmen learning and executing their duties as "cyber wingmen," just how much does the typical airman really know about what to do to ensure networks are secure and information is protected? Do airmen have a foundation of knowledge on the vulnerabilities of networks? If not, then maybe the question really is, "how *relevant* is network security to that airman?" Air Force culture today indicates that most airmen do not know that much about network security, nor do they feel that it is relevant (Courville, 2007). There are many reasons that airmen do not consider the importance of network security and the discussion begins with a closer look at culture in today's Air Force.

3.7 Squadron Culture

> *We can prevent these events with due consideration and proper procedures, but in the past, we've regarded network protection and security as the "comm guy's job", and as a user inconvenience. This must no longer be the case.* (Schwartz, 2009).

The first issue is that cyberspace and network security are not the primary concern in the majority of squadrons in the Air Force; rather cyberspace *supports* the mission. The Air Force didn't build a vast, interconnected network just to secure and defend it; the network was built in order to support the primary missions of units throughout the Air Force. With that in mind, it is fair to say that airmen do not arrive at work each day prepared to defend the network – they are there to accomplish their respective mission. So computer and networks represent a means to an end. When airmen therefore turn a blind eye to network security, they do so because the focus is on the grander mission vice tools used to accomplish that mission.

Second, it is very easy for airmen to characterize network security as a barrier to mission accomplishment. “Each layer of security to prevent unwarranted intrusions is also a potential barrier to the efficient operation of a cyber system” (National Security Threats in Cyberspace, 2009). As bureaucracy expands into the far reaches of everyday life in a given unit, this has a tendency to create a default attitude in units that *all* procedures, rules, and processes are bad. Therefore in units where barriers to mission accomplishment exist, which is to say all units in the Air Force, the ease with which airmen arrive at a negative connotation for just about any given rule is rather swift.

Third, a “general lack of security culture” exists at the unit level in the Air Force (Courville, 2009). Although attacks on government and military networks reach the news, such as those against U.S. and South Korean government websites in July 2009, the issue does not seem to garner enough attention to jumpstart cultural change. It seems that the lack of any significant, tangible damage or loss of life causes airmen to be nonchalant about network security. Airmen tend to have the attitude that it is someone else’s job to secure the networks. This is a side-effect of the centralized control of networks as discussed in the previous section, and the tendency to keep users in the dark about security concerns, which will be discussed in the later.

With this basic understanding, the discussion now moves on to more closely look at the effect of network security on end users, probing for an answer to the question, *who ultimately bears the cost of network security?*

3.8 Effect of Network Security on End-Users

> *I know, up on top you are seeing great sights, but down here at the bottom we, too, should have rights.* (Dr. Seuss, 1958)

In Dr. Seuss' story *Yertle the Turtle,* the main character is driven to expand the kingdom that he rules (1958). To do this, he orders turtles to stack themselves on one another to create a perch and thus enable him to sit higher and see further. The king is happy with the result as he can now claim to rule everything below him and as far as they eye can see. What the king fails to understand is the fragile nature of his construct which places heavy, undue strain on those individual turtles below him that are neither equipped nor motivated to remain in their posts. So what does this have to do with network security? In many ways, the nature of cyberspace places a similarly heavy burden on individual users at the lowest levels. It would be one thing if those users had a choice to use technology or not. In today's Air Force, IT is increasingly forced on end users. Even though users have no say in many of the technological systems implemented today, the Air Force demands that they use them while avoiding vulnerable procedures and practices. Just as the turtles in the story above, end users are often not equipped or motivated to carry the burden of IT systems. This section is intended to provide justification for the claim that it is the end user that pays the price for network security. "Security always creates a cost of some sort, and that cost will need to be borne by some actor in the system" (National Security Threats in Cyberspace, 2009).

Network security is often implemented with a "defense in depth" concept. Using this model, network defense represents layers of security. For example, firewalls implemented at the edge to isolate networks or sub-networks will be one layer. An additional layer can be provided by anti-virus software on a client workstation. The idea is that security layers, synchronized and managed well, will be able to negate most attack vectors through redundancy. If the firewall does not block it, then the anti-virus software will, etc. However, these layers of security can very quickly become complex and cumbersome. “Typically, user interfaces accompanying security features are awkward. As a result, the secure systems are more difficult to use than the nonsecure systems” (Hundley and Anderson, 1997). Because of the added strain on resources, the effect can be felt by those end users at the network edge. Therefore, the cost to the end user can range from slow, inefficient processors to denial of service.

Another strain that is placed on end users involves the inherent vulnerabilities of software. Obviously, there is a valid need to keep software up to date with necessary patches that fix or mitigate vulnerabilities. And end users typically will not complain about the fact that software needs to be fixed. The problem lies in communication and methodology of software patching. In the best case scenario, network administrators would install necessary fixes when it least affects the mission. In some cases this happens. A base-wide e-mail might remind airmen to log off or restart their computers at a certain time, typically at the beginning or end of their duty day. All is well as long as there is minimal impact on the mission. Conversely, the worst case scenario would be that software patches are not communicated and are conducted at a time which does have an impact on the mission. In this case, airmen feel the full effect of network security when a critical system is unusable for a significant amount of time while it is loaded and configured with appropriate software patches. Meanwhile the clock is ticking on the unit’s mission. Some airmen will find tasks which do not require a computer to occupy their time, others simply may not have that luxury. Therefore, the cost to these end users is time lost waiting on necessary software patches.

An additional layer is end user security, through training and education. One would think that the education of users on security concerns would be a principal concern. Surprisingly, the opposite is the case. Empirical evidence suggests that in the field of network security, the consensus is that users should be kept in the dark, for the sake of the network. In his article, *The Six Dumbest Ideas in Computer Security*, Marcus Ranum ranks “Educating Users” as the fifth dumbest idea, stating that, “a significant percentage of users will trade their password for a candy bar” (2005). Furthermore, strategies that include educating end users are met with cringes and winces by network administrators who have tried educating users only to find that it is “largely futile” (Schneier, 2006). Even considering the vulnerable nature of technology, with more vulnerabilities discovered each day, there is little concerted effort to get the end user “buy-in” that is so desperately needed for security to improve. The Air Force’s annual online information assurance training then looks more and more like a placeholder designed to give the impression that a legitimate program exists for user education.

The fundamental exemplification of the weakness of end users is the action of simply opening an infected attachment or link sent to them in an e-mail, perhaps as part of a phishing attack. Obviously there will be some end users who will be unable to show restraint and will click the attachment or link, thereby releasing an infection of some sort into the network. Notwithstanding the consequences of this action (mindful that it can be catastrophic), how much is done to provide immediate feedback to the end user who committed the offense? While focused efforts to contain the infection and perform necessary patches and repairs will ensue, it is likely the end user will never know the full consequences of his or her action. Even in cases where a reprimand is handed out to the offender, it is unlikely that the response to the incident will include requisite instructional fixes that speak to the specifics of the incident – why it was bad, what effect it had, and how to prevent it in the future. The end user is left with a basic concept that network security is important, but will have gained nothing in the form of specific knowledge that can help promote network security. Schneier summarizes the cost to end users as the paradox of industry which has, "convinced people they need a computer to survive, and at the same time they've made computers so complicated that only an expert can maintain them" (2006).

Furthermore, is the action of the end user in the above scenario really the *root cause*? What is the answer when the user asks, "why did the e-mail arrive in my inbox with malicious code attached in the first place?" "Computers need to be secure regardless of who's sitting in front of them" (Schneier, 2006). The idea that hardware and software are inherently insecure suggests that the root cause does not lie with the end user. Then, why are they repeatedly singled out as the "weakest link"?

In truth, the attitude and actions of end users are very difficult to defend, particularly when catastrophic security violations occur due to error, mistakes, or bad judgment. But, once again, these are the airmen on the "front lines of cyberspace." Clearly, education on the intricate details of network security is not a viable option, but then again neither is reliance on annual IA training. Perhaps the balance lies somewhere in between, such as the inclusion of airmen in an integrated, team effort designed to mitigate the risk of network threats.

In summarizing the effect of network security, the cost to end users is stemmed in the requirement to keep networks safe through layered security, vulnerable software that regularly requires patches, and the complicated nature of computers that makes education of users a challenge that most would rather not undertake. While the end users clearly pay a price for network security, it is just as important to note the additional effects on the mission.

3.9 Effect of Network Security on the Mission

Further creating a barrier to communication between network administrators and end users is the often nebulous concept of the mission. Network administrators want desperately to support the mission, and some feel that the logical way to do this is to have the end user "teach" the needs of the mission in order to convey priorities, essential processes, etc. Sadly, this is an unfortunate misconception. The mission is just not that easy to teach. To explain this, two distinct characteristics of the mission at the unit level should be addressed.

First, the mission is dynamic. Although this is a simple statement, it is enormously important. To illustrate, take a flying unit that is tasked with a flying schedule consisting of ten sorties on a given day, and further assume that this squadron is at home station conducting peacetime training. This flying schedule will likely include several different types of sorties designed to accomplish training events for the aircrew. Now say a guest arrives at the unit requiring information as to what the priorities for the squadron are for that specific day. No doubt the officer in charge of operations will likely have a set of "marching orders" from his or her leadership that dictate which events have highest priority, in the event of broken aircraft, fallout, inclement weather, etc. These priorities represent the dynamic mission of the unit – on that specific day as it relates to that specific schedule.

Now suppose that the exact same schedule of ten sorties is tasked the subsequent day, with all the players in the exact same position as the previous day. Is it safe to assume that the priorities will be the same? Those experienced in the conduct of training operations in a flying squadron will emphatically say "no." Why? From one day to the next priorities change for a variety of reasons. Perhaps one sortie in particular, with no change to their apparent tasking on the schedule, is assigned to support critical training requirements for an outside agency. Or perhaps, in that one day's time, an individual was tapped for a short notice Temporary Duty (TDY) assignment the following week and now needs some critical training event. These are just a couple of factors that can lead to monumental changes in priorities – which again represent the dynamic mission.

The second important characteristic of the mission at the unit level is, at the risk of sounding obvious, that it relies on information. That is to say, it relies on the logical delivery, conveyance, and control of information. This is cyberspace dependence, at its most basic level. In today's flying squadrons, operations can come to grinding halt if information services are denied or interrupted. To illustrate, take once again the example of the flying schedule of ten sorties discussed above and further assume that it is a squadron of F-15E mighty strike eagles. Each sortie has two aircrew assigned, for a total of twenty airmen tasked to fly. During the time these individuals are conducting their flight briefing, assume a critical read file is published which requires each aircrew to "sign off" in order to ensure compliance. The client server application, not to name specifics, for conducting this simple process of signing off the read file requires each aircrew log in *individually* – a necessary measure for network security. This program then essentially represents a choke point for the mission. Even if the program optimistically only requires one minute of time for each aircrew, that is 20 minutes total. This relatively small chunk of time, needed to pass critical information, can severely disrupt the mission. Even a seemingly innocent program designed to enable the logical control of information can become a barrier to mission accomplishment.

3.10 Barriers to Communication, revisited

Having now added to the discussion from the perspective of the end user and the mission, the barriers to communication between network administrators and end users continues to get further restricted. First, the cultural issues introduced thus far represent the attitudes and ideals present in today's squadrons. Second, the dynamic nature of the mission and its strict information requirements provide additional obstacles of uncertainty and conflict. Seen together, all these barriers form a difficult puzzle for network administrators and end users to solve (Figure 3).

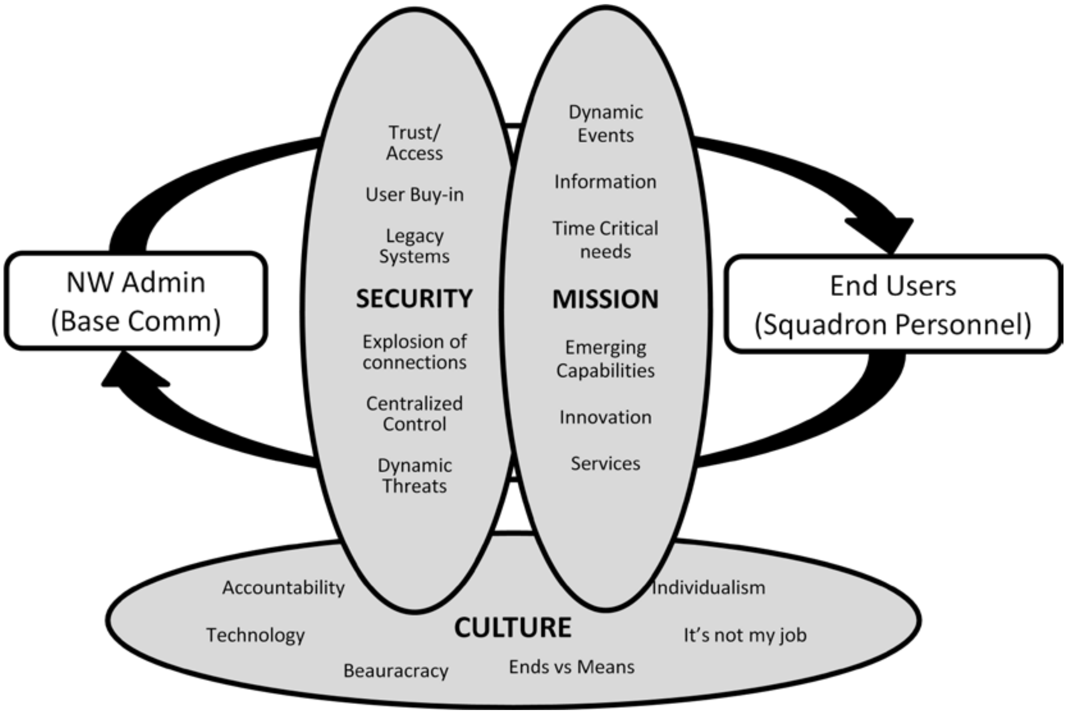


Figure 3. Barriers to Communication, revisited

It is clear that the relationship between network administrators and end users is constrained by a myriad of obstacles. Given that many of these issues are evolving trends – centralization, emerging technologies, attack vectors, etc. – this problem stands only to get worse. The Air Force must initiate action aimed at mitigating the effects of the barriers to communication.

Network security is ultimately a team effort and this paper thus far has attempted to provide some insight into issues that inhibit airmen from truly realizing the full capabilities of cyberspace because of strained relationships and a lack of accountability. It is with the team concept in mind that this paper will now attempt to develop solutions to the problems created by cyberspace dependence in Air Force squadrons.

IV. Cyber Program for Air Force Squadrons

> *The commander who knows his "human" systems but who does not understand his "automated" systems will be vulnerable to surprise - possibly to defeat.* (McKitrick and others, 1998)

This paper has attempted to highlight some of the issues that flying squadrons face in dealing with an ever-increasing dependence on cyberspace. The culture of flying organizations, specifically the issue of accountability, is a critical concern for leaders to consider when implementing changes that place greater emphasis on computers and networks. The fragile relationship between end users and network administrators is another concern that will play an important role in the future fighting force. Having discussed the key issues, it is now time to lay the framework for the solution set identified in this paper.

The purpose of this chapter is to present the case for establishment of a Cyber program in flying squadrons. This program will take on a similar structure to that of existing Force Protection (FP) and Safety programs. An important part of the program is the appointment of a squadron Cyber Officer who will serve as the unit liaison with the evolving cyberspace community (base comm, network administrators, etc.). Additionally the Cyber Officer will provide an advocate for unit personnel on cyberspace related issues, and oversee the integration of new IT systems into unit operations.

Before delving into the details of the Cyber program, it is first necessary to take a closer look at historical perspectives that a Cyber program should be modeled after. FP and Safety are two specific programs whose structure and history can be logically used to develop the Cyber program model.

4.1 Force Protection

> *On 25 June 1996 a terrorist attack upon US forces deployed to Dhahran, Saudi Arabia resulted in nineteen fatalities and numerous injuries. The Khobar Towers tragedy serves as yet another grim reminder of the increasing vulnerability and likelihood of attack on US forces in garrison both abroad and potentially at home.* (Creamer and Seat, 1998)

4.2 Background

Prior to the attack described in the excerpt above, at least three other incidents shared similar characteristics - the 1983 attack on the barracks in Beirut, the 1993 World Trade Center attack, the 1996 Oklahoma City bombing (Lafrenz, 1999). However, it was not until the Khobar Towers attack that the Air Force got serious about defining and implementing a formal FP program. Many problems hindered the development of the FP program – no one knew who exactly was in charge, the role of different agencies was unclear, and most individuals did not have a clear understanding of the threat. As the program evolved there were disagreements over vulnerabilities and priorities. It was also clear that without a definitive strategy, efforts to defend people and resources would be challenging. This section will provide a brief synopsis of FP development.

4.3 Key Features

> *Mitigating the issues of the Force Protection program begins with clear articulation of what leadership expects*. (Lafrenz, 1999)

Responsibilities and Authority. In *Doctrine (Maybe), Strategy (No) Will the Air Force Implement a Force Protection Program?*, James L. Lafrenz studies the aftermath of terrorist attacks leading up to and including Khobar towers (1999). His critical analysis provides learning points that shaped the FP program. Lafrenz places heavy emphasis on establishing clear responsibilities and authority. Both the military and government sponsored investigations into the events leading up the Khobar Towers attack revealed a common theme – that numerous questions existed among key actors which suggested confusion and turmoil over the safety of troops from terrorist attacks. Who is in charge? Which agency should be responsible for what? What is the threat? In the case of Khobar towers, vulnerability assessments had repeatedly highlighted the threat of a penetration or proximity bomb against the facility; however, coordinated efforts had failed at moving the perimeter fence further from the building (Creamer and Seat, 1998). Also, consideration had been given to moving airmen to another facility, and the installation of an evacuation alarm was lost in bureaucracy (Creamer and Seat, 1998). This pattern suggests that information was available and efforts to integrate and coordinate actions among agencies were stymied due to a lack of clear responsibility and authority.

Of critical importance is the relationship between key actors: security forces (SF), civil engineering (CE), explosive ordnance disposal (EOD), medical personnel, etc. Lafrenz report written in 1999, noted that, "To date, the Force Protection initiative is simply a collection of parochial activities by individual Air Force organizations without the integration of the resources necessary to counter a common threat." Over time, agencies developed a better understanding of their roles and responsibilities. This was made possible through the establishment of a focal point that serves as the coordination element (Figure 4). Under the guidance of doctrine, Air Force wings, groups, and squadrons established a FP officer, a designated position at the wing (or installation) level. This office then extended its oversight through representation of similar FP officers or NCOs throughout each unit on a given base. Each wing also developed their own FP procedures – since again its focus is primarily at the installation level.

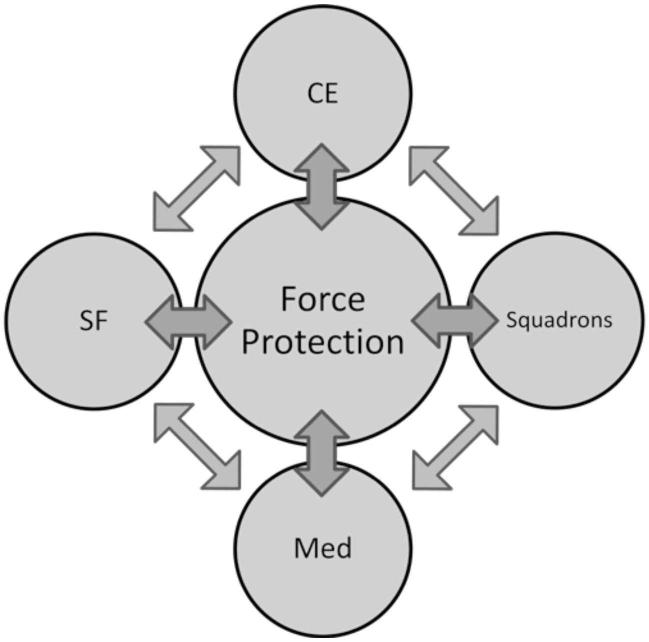


Figure 4. Force Protection Focal Point and Integrated Effort

Supporting organizations (civil engineering, security forces) were absolved of central authority meaning they could remain active participants without the baggage of another time consuming additional duty. Finally, the FP message was disseminated across the Air Force to all airmen. The "Eagle Eyes" program is an example of the emphasis on FP which enlists the participation of all airmen to be alert and attentive to potential threats to personnel, assets, and capabilities in both peacetime and wartime.

Priorities and Strategy. Strategy that shaped the FP program offers insight into the priorities of the program and the importance of interagency relationships. A closer look at Doctrine that defines FP is thus warranted. Air Force Doctrine Document (AFDD) 2-4.1 states, "the essential goal of force protection is to counter threats against

Air Force personnel and assets" (2004). The central themes derived from the FP doctrine are founded on the principle of protecting the Air Force's "personnel, assets, and capabilities" (AFDD 2-4.1, 2004). AFDD 2-4.1 further states that FP is inherently based on integrated actions "throughout the spectrum of peacetime and wartime military operations" (2004). The cumulative effort results in a FP program that responds to threats and vulnerabilities through continuous risk assessment and analysis (AFDD 2-4.1, 2004). The themes found in FP doctrine suggest that the delineation of priorities allows the program to be transparently applicable across the entire Air Force. It also stresses the importance of interagency relationships and their pursuit of a common goal.

4.4 Organization and Reporting Structure

Of course, for all the trials and tribulations that hindered the development of FP, today the program is embedded in Air Force operations. AFDD 2-4.1 states that, "Force protection is an inherent responsibility of command. Accordingly, commanders at all levels must make Force Protection an imperative" (2004). With regards to the organizational structure, AFDD 2-4.1 instructs, "Commanders should also appoint a single FP local point, an individual trained and versed in FP issues and methodologies with appropriate rank and experience, to act as their advisor on all FP issues" (2004). The following notional structure (Figure 5) is based on the recommended structure in AFDD 2-4.1 which highlights the importance of the FP program.

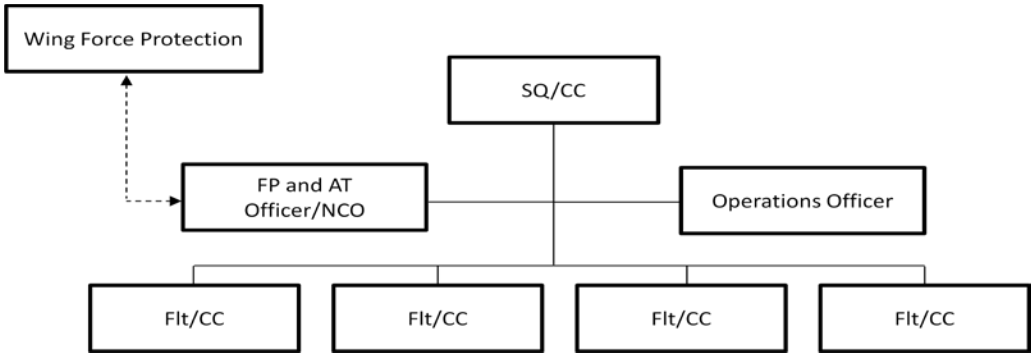


Figure 5. Force Protection Organizational Structure

A couple of key features in this depiction are worth noting. Notice the FP officer reports directly to the commander. Notice also the communication channel between the squadron FP officer and the Wing FP office. This type of structure emphasizes the importance of the program. FP is a commander's program since it directly affects the mission, not only in deployed combat settings but also in peacetime at home station. Therefore, the FP officer is an active member of the commander's staff. This structure also enables the dissemination of information from the central wing office through the squadron representatives, which serves to include all airmen as active participants.

4.5 Safety

> *If an airplane crashes, if a ship runs aground, if a tank goes off the road and rolls inverted into a ditch, what is one of the very first things commanders do? They stand up investigation boards or mishap boards because they want to get at the root cause of the problem and fix it. Commanders study the causes, they develop lessons learned, they promulgate them through training, and they make sure the force learns from the mistakes. Then they determine the right level of accountability.* (Chilton, 2009)

4.6 Background

The Air Force Safety program is recognized as an effective means for mitigating circumstances for the greater good of personnel, assets, and capabilities. Through a strong culture of safety awareness, the Air Force identifies factors that pose a significant risk to resources. Through effective leadership and communication channels, the Air Force implements policies and procedures designed to protect personnel and resources. Within the realm of Safety, of particular note is the community of Aviation Safety. This section begins by exploring the underlying culture that serves as the basis for safety programs, and also addresses the specific features of Aviation Safety.

4.7 Key Features.

> *Safety culture is the enduring value and priority placed on worker and public safety by everyone in every group at every level of an organization. It refers to the extent to which individuals and groups will commit to personal responsibility for safety, act to preserve, enhance and communicate safety concerns, strive to actively learn, adapt and modify (both individual and organizational) behavior based on lessons learned from mistakes, and be rewarded in a manner consistent with these values.* (Wiegmann and others, 2002)

Safety Culture. The excerpt above suggests that Safety culture is successful in organizations because of the far-reaching effect of member "buy-in." That is, all members of the organization commit to be an active participant. Consider the following list (Figure 6), which provides additional thoughts on Safety culture.

- Safety culture is a concept defined at the group level or higher, which refers to the shared values among all the group or organization members.
- Safety culture is concerned with formal safety issues in an organization, and closely related to, but not restricted to, the management and supervisory systems.
- Safety culture emphasizes the contribution from everyone at every level of an organization.
- The safety culture of an organization has an impact on its members' behavior at work.
- Safety culture is usually reflected in the contingency between reward systems and safety performance.
- Safety culture is reflected in an organization's willingness to develop and learn from errors, incidents, and accidents.
- Safety culture is relatively enduring, stable and resistant to change.

Figure 6. Safety Culture (Wiegmann and others, 2002)

Certain themes can be drawn from this representation of Safety culture – it requires participation of all organization members, it is truly concerned with improving conditions to avoid accidents or catastrophes, it is a learning process. With this in mind, the principle characteristic of Safety as a learning process will be discussed specifically as it relates to the field of Aviation Safety.

Organizational Learning. When studied as an organizational learning model, military Aviation Safety is an interesting subject. As Figure 7 illustrates, of particular note is the phenomenon between 1975 and 1995 when military aviation mishaps decreased steadily from 309 to 76, and fatalities dropped from 285 to 85 (General Accounting Office, 1996).

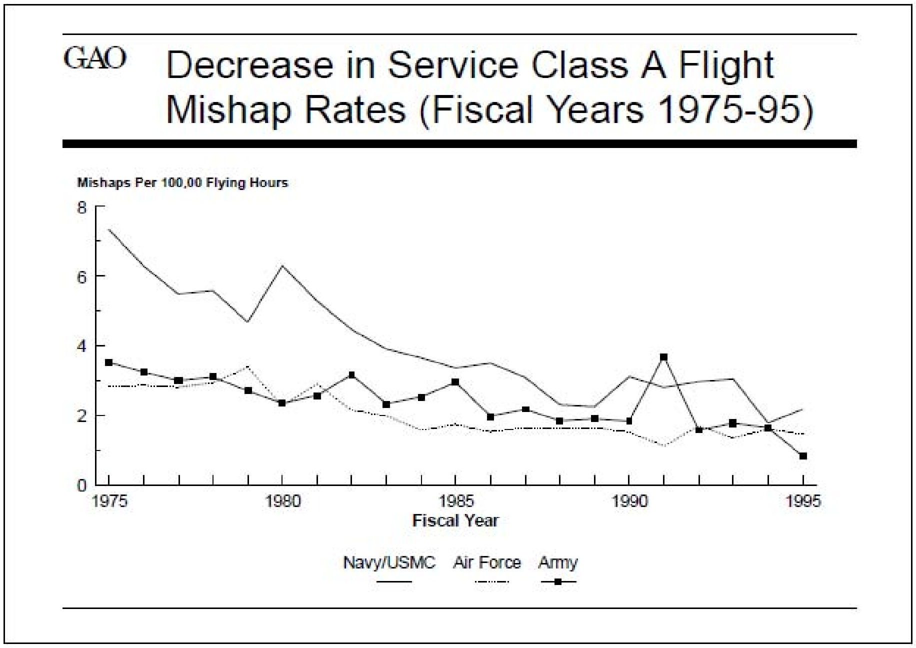


Figure 7. Decline of Aviation Mishaps (GAO, 1996)

What happened in military aviation that caused such a drastic, but welcome, decline? Those years represent a time of exponential *increase* in aviation, so how can the disproportionate *decrease* in mishaps and fatalities be explained?

Ballesteros offers that the contradiction between the danger intrinsic to aviation and the low number of accidents can best be explained as “the accumulated result of intense [organizational] learning” (2007). The field of Aviation Safety sets an interesting precedent here – that an emphasis on organizational learning can have a profound effect on a discipline that seems largely uncontrollable. The General Accounting Office (GAO) Report identifies the Air Force’s efforts to track safety recommendations, disseminate safety information, and undertake special initiatives as contributing factors to the improvements in Aviation Safety (1996).

4.8 Organization and Reporting Structure

The organizational structure of the Safety program (Figure 8) is nearly identical to that of the FP program discussed earlier. In a flying squadron, the commander assigns the Safety Officer from among his personnel at his or her discretion. The squadron Safety Officer – usually a mid to senior Captain in most flying squadrons – is provided a short training course that outlines his or her duties as the unit safety representative. This is a critical feature of the safety program – there is no need for previous expertise since the individual is provided the necessary tools to perform their job after having been identified as a candidate for the position.

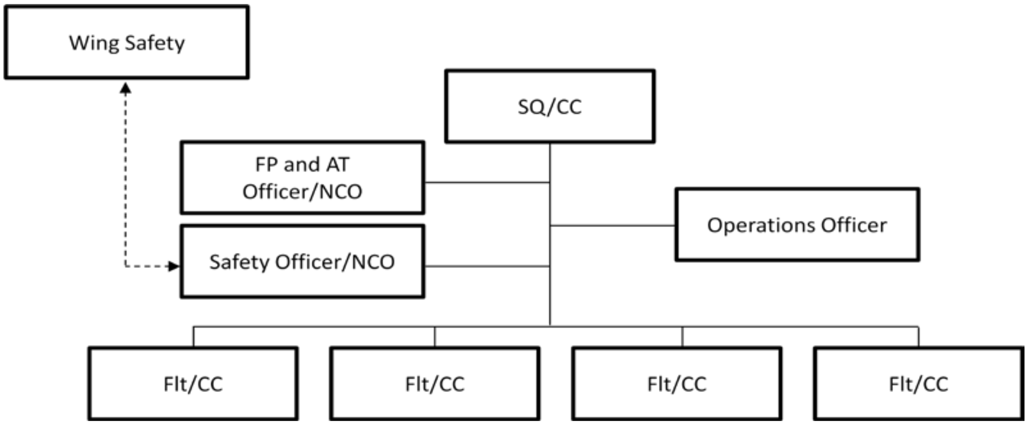


Figure 8. Safety Program Organizational Structure

The unit Safety officer is an advisor to the commander on unit safety issues, disseminates information as directed through safety channels, and provides an advocate for unit personnel who have concerns or recommendations about practices and procedures in the workplace. Notice this type of communication channel is similar to that of the FP program. This practice of reporting concerns and recommendation, with an emphasis on organizational learning, is another key feature that warrants further detail.

Incentive and Non-retribution. The communication channel between the Safety Officer and any individual who has a concern or recommendation is a unique characteristic. Individuals have the opportunity to report on any safety related issue without the threat of immediate retribution. Of course, anyone who commits a crime or egregious safety violation may face punishment in due time. But the important aspect here is that safety communication channels are meant to be open lines for members at any level to bring up those concerns or incidents that they feel warrant attention.

To illustrate, consider an airman who has identified a hazardous condition on the flight line. The airman notifies the immediate supervisor who replies that it is not a big deal and refuses to do anything to correct the condition. The airman can report the condition to the Safety Officer without the threat of retribution from the supervisor. This communication feature of the Safety program is noteworthy in that it provides an incentive for airmen to report what they see. In essence, the Safety program is a system of "checks and balances" to overcome obstacles, such as the supervisor who refuses to fix an unsafe condition. Because the Safety program is built on the premise of learning from incidents and recommendations, anyone can contribute to the program by simply highlighting the issues they have discovered.

FP and Safety programs provide unique models that can be used to build a framework for a Cyber Program in Air Force flying units. The key features described in the previous sections can be pooled together to formulate the ideals that should shape the future unit level cyberspace liaison element.

4.9 Lessons Learned from Force Protection and Safety Programs

FP highlights the importance of establishing clear roles and responsibilities. Do today's key cyberspace organizations have questions about their roles and responsibilities? At the unit level, roles and responsibilities are either significantly unclear or do not exist. Squadron leadership leans on resident expertise (provided such expertise exists) and is happy to avoid cyberspace issues as long as the network is functioning and the mission is not directly affected. An underutilized CSA career field is available to respond to incidents and requests for help in the unit; however, CSAs lack the administrator privileges to do much other than call the next person. Airmen have an indifferent attitude about network security, and do not see themselves as having an important role in cyber defense. All this justifies the need to establish clear responsibilities and authority.

The FP program also stresses the importance of priorities and interagency relationships. Today, the way cyberspace is used to accomplish the mission in one unit could be vastly different than in another – leading to a varied affect on mission assurance. If the priority of one organization in particular is to protect our networks, then is that in spite of, or in concert with wing, group, and squadron missions? Certainly, organizations or efforts that currently integrate cyberspace operations, across the spectrum of peace and war, in order to respond to threats are difficult to find. Without a coherent strategy, it is difficult to find a common picture for which the Air Force to base its priorities.

The Air Force Safety program has been successful in mitigating the risks associated with aviation. At the heart of Aviation Safety is the concept of intense organizational learning. Imagine a similarly constructed Cyber program that places emphasis on intense organizational learning. The subsequent side-effects of this program, that directly impacts the daily cyberspace practices of airmen, could have a similarly profound effect on mission assurance in Air Force squadrons. This program would require signification attention from leadership in addition to the “buy-in” of organization members as discussed earlier. The attention given to safety in the Air Force suggests monumental emphasis by the highest levels of leadership. For Air Force leadership to maintain this type of oversight, there must exist an effective reporting structure to enable communication down to the unit level.

In order to learn from events, the Safety program features open lines of communication designed to encourage airmen to participate. Currently, there exists no such open line of communication nor incentive within Air Force squadrons for individuals to report cyber related incidents. On the contrary, “there are huge disincentives to reporting cyber intrusions” (National Security Threats in Cyberspace, 2009). An airman who mistakenly opens a malicious e-mail attachment would rather pull the plug on the infected system and quickly vacate, lest they receive blame for making an innocent, or not so innocent, mistake. Just as with aviation mishaps, much can be learned from each and every incident involving the misuse or attack of IT systems, yet there is no concerted effort to emphasize such incidents. Whereas aviation safety has saved lives, an effective program of the same magnitude could not only ensure the mission at the unit level, but also have strategic implications network security in the Air Force.

4.10 Proposed Squadron Cyber Program

> *It is not clear, as a result, that today's military organizational structure is the best way to manage the complexities of information warfare as it might unfold in 2020. (McKitrick and others, 1998)*

It is the assertion of this research that a Cyber program constructed similarly to FP and Safety programs would enhance the mission in Air Force flying units. By emphasizing the importance of cyberspace operations through the dissemination of information and by giving commanders a focal point for cyber related issues, flying squadrons will be better equipped to integrate cyberspace into their daily operations.

The solution proposed in this research boils down to the idea that every unit in the Air Force appoints an individual to manage and oversee the FP program, and similarly, every unit has a Safety Officer. Does it not make sense to then have a similar Cyber program and Cyber Officer? The success of the other programs discussed hinged on commitment from Air Force leadership, emphasis on learning, and establishment of clear goals and objectives. The squadron Cyber program should be built on those same principles.

4.11 Purpose of the Cyber Program

The purpose of the squadron Cyber program is to provide advocacy and leadership to integrate cyberspace into squadron operations. A squadron Cyber officer serving under the auspice of the greater Cyber program will become the linchpin for units to fully realize the capabilities of cyberspace operations. This program can have a positive effect on Mission Assurance by establishing clear roles and responsibilities, opening communication channels, and gradually creating a culture of cyberspace awareness among airmen.

4.12 Key Features based on Force Protection

The strategy and priorities of FP, when amended to mirror the attributes of cyberspace operations, are the foundation of the proposed Cyber program. Based on FP Doctrine, the essential goal of the Cyber program shall be to counter threats against Air Force personnel and assets. Likewise, Cyber programs will emphasize integrated actions throughout the spectrum of peacetime and wartime military operations. Finally, the cumulative efforts of the Cyber program should be to respond to threats and vulnerabilities through continuous risk assessment and analysis. These statements represent strategic guidance that will serve as the groundwork for the principles of the Cyber program.

Of critical importance is the establishment of clear roles and responsibilities among key actors. Based loosely on the agencies that constitute and support the FP program, the following general statements should provide the basis for role establishment. Squadron leadership will ensure a fundamental awareness of cyberspace operations and maintain close visibility on both equipment and practices. The squadron Cyber officer will be the primary focal point for all cyber related issues in the unit. He or she will advise the commander on these issues and will serve as a direct liaison with cyberspace organizations (base comm, network administrators, etc.) in order to disseminate information, collect and track incidents and recommendations, and establish initiatives to improve cyberspace operations. Unit CSAs should fall under the squadron

Cyber officer and will maintain oversight over equipment inventory, computer system procurement, and general IT procedures and practices in the unit. Squadron intelligence personnel should support the Cyber officer by conducting regular cyberspace-specific threat briefings. The Cyber officer should also work closely with the unit FP officer since the goal of both functions is to protect personnel, assets, and capabilities. Lastly, but certainly not least, airmen must know their role as operators in cyberspace, which will be discussed in more detail later.

4.13 Key Features based on the Safety program

Of the many key issues that will challenge the proposed Cyber program, establishing a culture of cyberspace awareness is perhaps the most daunting. Culture transformation is not an easy task, and certainly shaping attitudes of airmen to effectively participate on the "front lines of cyberspace" will prove a monumental feat. As with Safety, this begins with significant "buy-in" among organization members. To do this, squadrons must establish clear goals and objectives that stress safety and security of cyberspace operations which support the unit's mission. Personal and unit accountability is a key area of concern. Commanders must develop unit specific cyberspace policies and enforce them! Airmen should be afforded open communication with the Cyber officer that provides both non-retribution and incentive for reporting suspicious behavior, user errors, broken or malfunctioning equipment, etc. Squadrons must also be willing to develop and learn from cyberspace related incidents – which suggest both a culture of open communication, and organizational learning.

In order to foster an atmosphere of organizational learning, the Cyber Officer will build a model based on the Safety program to disseminate information on current cyber topics, track recommendations and incidents, and develop training tools to educate squadron personnel. The unit cannot learn from previous incidents without a reliable and straightforward incident reporting process. Reporting procedures should offer airmen non-retribution when reporting errors and incidents (unless the violation is clearly egregious or unlawful). Without such incentive, airmen will be much less inclined to participate. By tracking and consolidating incidents, the Cyber officer can assess system and network vulnerabilities as well as deficiencies among unit personnel and develop commensurate training events in response to those deficiencies. An additional tool that may be beneficial is the concept of a squadron-wide Cyber Briefing, to be held quarterly, semi-annually, or annually. This regular Cyber Briefing will include a synopsis of the related incidents from the previous time frame, and provide unprecedented feedback on the key issues that the unit has experienced. This program should incorporate current intelligence on cyberspace issues throughout the local installation, and the entire Air Force and DoD. This formal venue can also serve as a springboard for new procedures, practices, or ideas that can improve the unit's capabilities.

4.14 Organization and Reporting Structure

It should be no surprise that the structure of the Cyber program will look strikingly similar to that of the FP and Safety programs discussed earlier. Indeed, the Air Force should avoid the temptation to start a new methodology from scratch and instead simply develop the program based on what already works. Figure 9 shows the proposed reporting structure at the unit level.

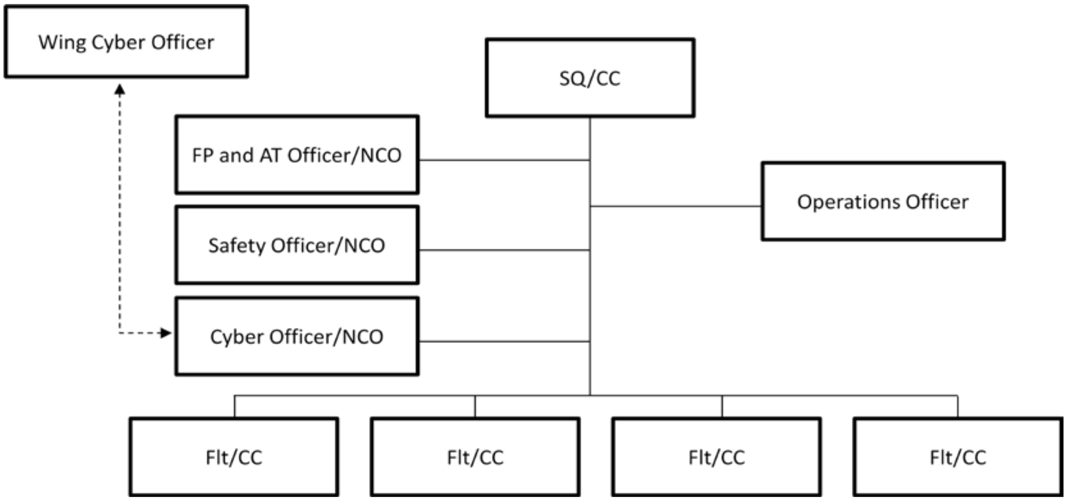


Figure 9. Proposed Cyber Program Organizational Structure

This structure takes the same approach as the previous models. The Cyber program is the commander's responsibility, since it ultimately affects mission assurance. Therefore, the squadron Cyber officer should be assigned to the commander's staff to report directly to and advise the commander on cyber related issues.

While it is relatively clear how the Cyber Officer fits among the unit staff, a separate discussion involves the reporting of the Cyber Officer up the Cyber chain – whatever that may be. Although many interesting solutions exist, the most practical application would be to mirror the relationship that developed through the establishment of the FP program. Specifically, this relates to the interagency relationship between the wing FP officer and the CE squadron commander. Many thought the CE commander would be the best fit to simply take on the role of wing FP. Lacking the necessary training, resources, and time, the CE commander was eventually absolved of being the FP focal point. Additionally, since FP is a commander's concern as it directly affects the mission, it made sense to establish a separate FP functional area with a dedicated FP officer. With the formal establishment of a FP officer, the two agencies built a working relationship of support. The CE squadron builds the roads, buildings, and other facilities while the FP officer remains concerned with the protection of those assets.

Consequently, the best way to delineate duties at the wing level may be to establish a Cyber officer who conducts assessments and spreads the word, while the communications squadron remains concerned primarily with operation and maintenance of the networks (Figure 10).

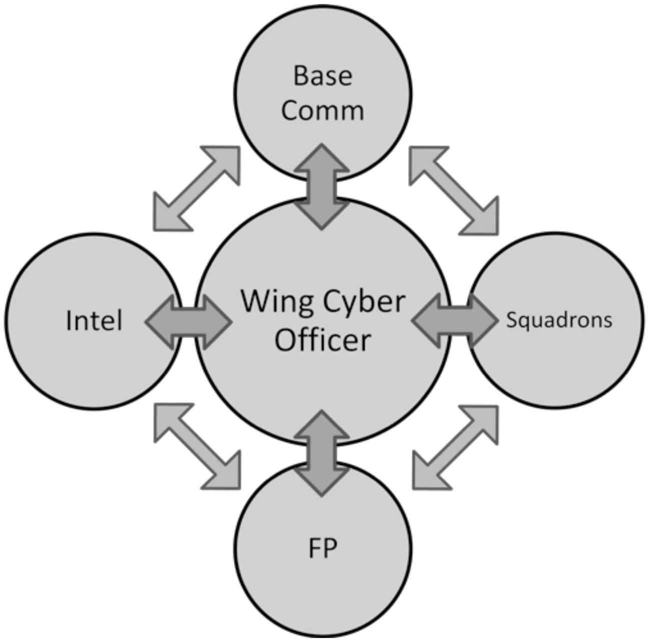


Figure 10. Wing Cyber Program Focal Point and Integrated Effort

4.15 Bridging the Communication Gap

> *Organizational change, then, is determined neither by the imperatives of the technology nor by the planned changes of organizational management. Instead, changes in work life are shaped (but not determined) by the prevalent discourses informing new technologies and the practices that emerge around them in actual workplaces. (Iacono and Kling, 2001)*

The creation of the Cyber program is intended to be a means to break down communication barriers and offer all parties an avenue to share and collect information. The squadron Cyber officer plays a key role, first, as a translator of end user needs, problems, and recommendations (Figure 11).

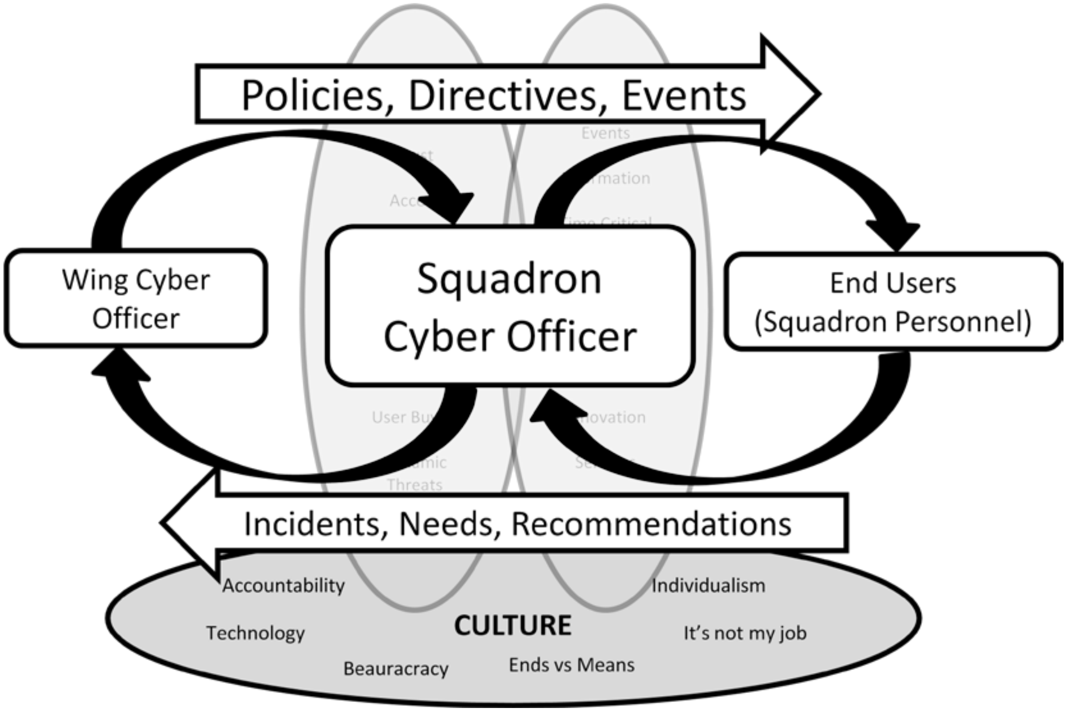
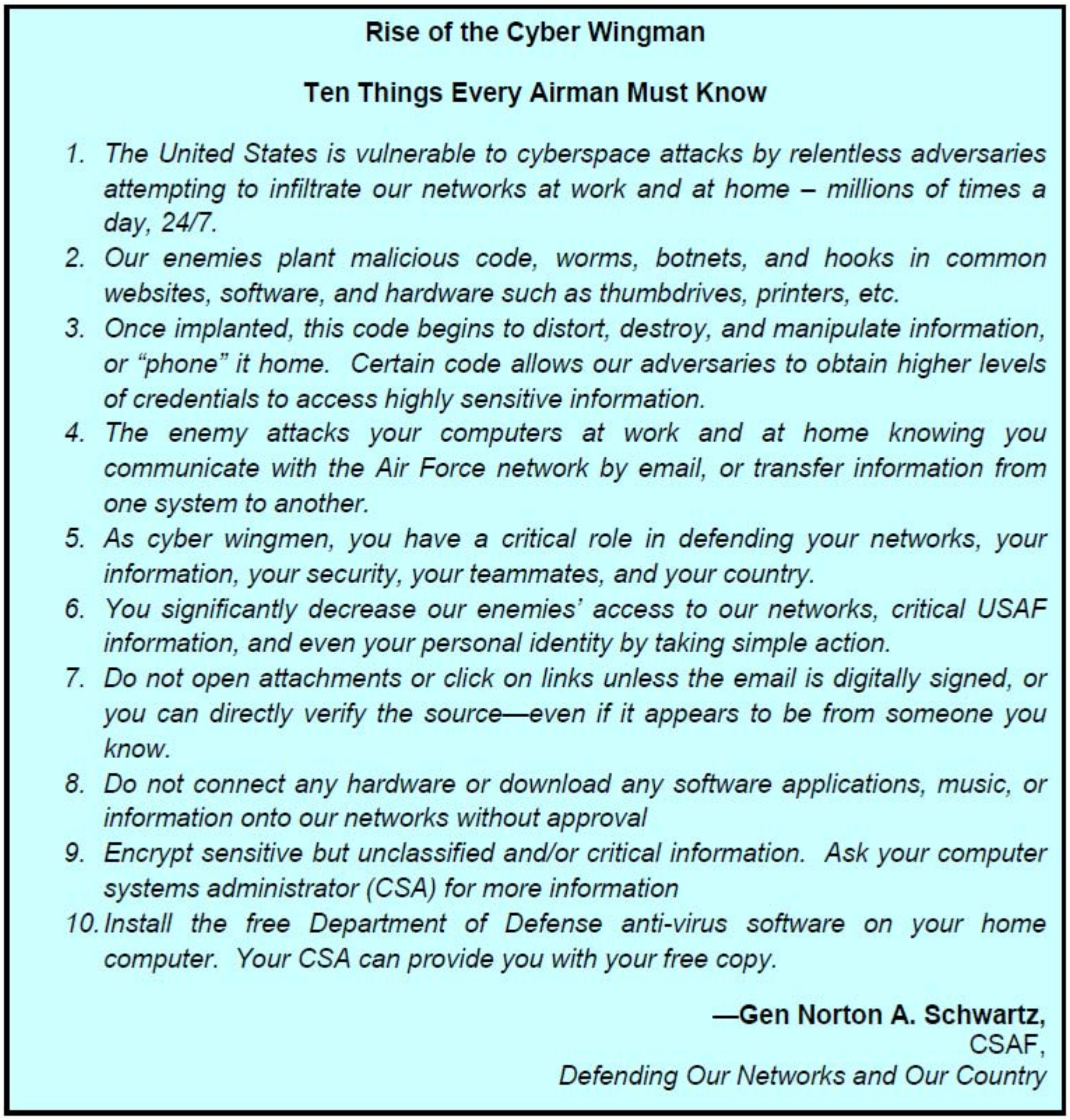


Figure 11. Bridging the Communication Gap

Second, provided the Cyber officer is trained and well versed in the basic nature of network operations this individual will be able to convey policies, directives, and information on network events to end users in order to bridge the communication gap.

4.16 Rise of the Cyber Wingman

The establishment of the Cyber program in flying squadrons in the Air Force will significantly impact the combat capabilities of these units. This program will emphasize cyberspace awareness and network security on the "front lines of cyberspace." In addition, this program will provide an advocate for war fighters who represent the end users. Finally, this program will go a long way towards bridging the communication gap between network administrators and end users. Ultimately the solutions presented in this paper are intended to identify a means for the Air Force to better organize, train, and equip airmen to fully realize the capabilities of cyberspace. The principle objective should be to provide airmen with the tools they need to effectively operate as "cyber wingmen." It is no doubt with this concept in mind, that the Air Force recently released the following "Top Ten" list (Figure 12) to guide airmen in their efforts to continue to successfully integrate cyberspace into their daily operations.



Rise of the Cyber Wingman

Ten Things Every Airman Must Know

1. *The United States is vulnerable to cyberspace attacks by relentless adversaries attempting to infiltrate our networks at work and at home – millions of times a day, 24/7.*
2. *Our enemies plant malicious code, worms, botnets, and hooks in common websites, software, and hardware such as thumbdrives, printers, etc.*
3. *Once implanted, this code begins to distort, destroy, and manipulate information, or "phone" it home. Certain code allows our adversaries to obtain higher levels of credentials to access highly sensitive information.*
4. *The enemy attacks your computers at work and at home knowing you communicate with the Air Force network by email, or transfer information from one system to another.*
5. *As cyber wingmen, you have a critical role in defending your networks, your information, your security, your teammates, and your country.*
6. *You significantly decrease our enemies' access to our networks, critical USAF information, and even your personal identity by taking simple action.*
7. *Do not open attachments or click on links unless the email is digitally signed, or you can directly verify the source—even if it appears to be from someone you know.*
8. *Do not connect any hardware or download any software applications, music, or information onto our networks without approval*
9. *Encrypt sensitive but unclassified and/or critical information. Ask your computer systems administrator (CSA) for more information*
10. *Install the free Department of Defense anti-virus software on your home computer. Your CSA can provide you with your free copy.*

—Gen Norton A. Schwartz,
CSAF,
Defending Our Networks and Our Country

Figure 12. Top Then Things Every Airmen Must Know (AFDD 3-12 *Draft,* 2008)

V. Conclusion

> *As we increasingly assimilate information capabilities into our military structure and focus more and more on establishing and maintaining an "information advantage" as a war-winning strategy, we also change the vulnerabilities of US forces, and ultimately of the United States itself.*
> (McKitrick and others, 1998)

As the Air Force continues to learn how to fly, fight, and win in cyberspace, it is clear that IT will no doubt be a crucial enabler. Empowering airmen to meet these and future challenges will require them to use technology with a solid foundation on the underlying importance of network security, mission assurance, and overall cyberspace awareness.

This research is intended to spark long-term discussion on how to better equip the core fighting unit of the Air Force – the flying squadron – in the prosecution of current and future wars. As the premier maneuver element on the "front lines of cyberspace," the Air Force can no longer afford to ignore the simultaneously powerful capabilities and vulnerabilities that exist at the squadron level.

5.1 Future Research

Development of squadron level cyberspace policies. It is not an exaggeration to say that units in the Air Force typically do not publish or maintain any sort of cyberspace policies. This type of "acceptable use policy" will assist commanders in establishing guidelines for airmen as well as provide a tool for assessment of activities and capabilities. Without a benchmark by which to assess their airmen, the commander's ability to hold his or her airmen accountable is severely hindered. Focused research into the key elements of a typical squadron cyberspace policy with specific do's, don'ts, etc. will help mitigate the culture and accountability issues discussed in this paper.

CSA manning, roles, and responsibilities. The CSA career field plays a crucial role in cyberspace awareness at the unit level. This research only brushed the surface of the issues that plague this career field in particular. The centralization of CSAs, while necessary due to efficiency concerns and manning cuts, has only served to muddy the waters on their actual roles and responsibilities. The Air Force cannot continue to allow this career field to be underutilized as ad hoc CSS members, which negates their usefulness as IT professionals. Future research is necessary to establish clear roles and responsibilities of the CSA career field specifically as vital liaisons in units on the "front lines of cyberspace."

Modeling Cyberspace Doctrine after Force Protection. In researching FP as a learning model for the development of a Cyber program, the similarities were countless. One could practically execute a "find and replace" of AFDD 2-4.1 to replace Force Protection with Cyberspace Operations and the result would be a usable document to begin building a directive for cyberspace. Many of the elements that are on the wish list for cyberspace (organization and C2, interagency relationships, planning and execution) are already found in the daily practices of FP. A focused research project with the intent of outlining the many ways in which cyberspace is like FP would be a valuable learning tool for those developing cyberspace doctrine and procedures.

Trend towards Networked Organizational Structure. Much of the research material used for this paper indicated the traditional hierarchical structure of military organizations is antiquated and inefficient. Certainly much of the business sector is flocking towards org charts that look more like a spider web (with many interconnected nodes) than a command structure (with subordinates reporting to a single leader). An interesting subject for future research is a look at the organizational structure of the future fighting force. Will it remain command structured? Will it be a network diagram? What are the advantages and disadvantages of each? What role will technology play in defining the organizational structure of the future?

BIBLIOGRAPHY

Albanese, Robert. *Management: Toward Accountability for Performance.* Homewood IL: Richard D. Irwin Inc, 1975.

American Bar Association Standing Committee on Law and National Security, National Strategy Forum, McCormick Foundation. *National Security Threats in Cyberspace*. Workshop Report. Annapolis MD, September 2009.

Arquilla, John and David Ronfeldt. "A New Epoch – and Spectrum – of Conflict," in *In Athena's Camp: Preparing for Conflict in the Information Age*. Eds. John Arquilla and David Ronfledt. Santa Monica CA: RAND, 1997.

Ballesteros, Jose S-A. *Improving Air Safety through Organizational Learning: Consequences of a Technology-led Model*. Burlington VT: Ashgate, 2007.

Chilton, General Kevin P. "Cyberspace Leadership: Towards New Culture, Conduct, and Capabilities," *Air and Space Power Journal*, 23(3): 5-10 (Fall 2009).

Creamer, Robert L. and James C. Seat. *Khobar Towers: The Aftermath and Implications for Commanders*. Thesis, AU/AWC/082/1998-04. Air War College (AU), Maxwell AFB AL, April 1998.

Connors, Roger and others. *The Oz Principle.* Englewood Cliffs NJ: Prentice Hall, 1994.

Convertino, Sebastian M. and others. *Flying and Fighting in Cyberspace.* Maxwell Paper No. 40. Air War College (AU), Maxwell AFB, AL, July 2007.

Courville, Shane P. *Air Force and the Cyberspace Mission: Defending the Air Force's Computer Network in the Future*. Occasional Paper No. 63. Center for Strategy and Technology, Air War College (AU), Maxwell AFB AL, December 2007.

Department of Defense. *Joint Publication 3-0 Joint Operations*. 17 September 2006 Incorporating Change 2, 22 March 2010.

Fulghum, David A. "Cyberwar Takes Shape," *Aviation Week & Space Technology*, 170: 48-51 (January 2009).

General Accounting Office. *Military Aircraft Safety: Significant Improvements Since 1975*. Briefing Report to the Ranking Minority Member, Subcommittee on Military Procurement, Committee on National Security, House of Representatives. Washington DC: GAO, February 1996.

Harshberger, Edward and David Ochmanek. “Information and Warfare: New Opportunities for US Military Forces,” in *The Changing Role of Information in Warfare*. Eds. Zalmay M. Khalilzad and John P. White. Santa Monica CA: RAND, 1999.

Horton,Thomas R. *The CEO Paradox*. New York: AMACOM, 1992.

Hundley, Richard O. and Robert H. Anderson. “Emerging Challenge: Security and Safety in Cyberspace,” in *In Athena’s Camp: Preparing for Conflict in the Information Age*. Eds. John Arquilla and David Ronfledt. Santa Monica CA: RAND, 1997.

Iacono, Suzanne and Rob Kling. “Computerization Movements: The Rise of the Internet and Distant Forms of Work,” in *Information Technology and Organizational Transformation*. Eds. JoAnne Yates and John Van Maanen. Thousand Oaks CA: Sage, 2001.

Jabbour, Kamal. “The Science and Technology of Cyber Operations,” *High Frontier*, 5(3): 11-15 (May 2009).

Janczewski, Lech and Andrew Colarik. *Managerial Guide for Handling Cyber-Terrorism and Information Warfare*. Hershey PA: Idea Group, 2005.

Johnson, Michele E. *An Analysis of Role Conflict and Role Ambiguity Among Air Force Information Management Professionals*. MS thesis, AFIT/GIR/ENV/03-08. Graduate School of Engineering and Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2003 (ADA415222).

Lafrenze, James L. *Doctrine (Maybe), Strategy (No): Will the Air Force Implement a Force Protection Program?* Maxwell Paper No. 17. Air War College (AU), Maxwell AFB, AL, May 1999.

Leidigh, Christopher. *Fundamental Principles of Network Security*. White Paper No. 101. [W. Kingston RI]: American Power Conversion, 2005.

Libicki, Martin C. “Incorporating Information Technology in Defense Planning,” in *New Challenges New Tools for Defense Decisionmaking*. Johnson, Stuart E. and others. Santa Monica CA: RAND, 2003.

-----. “What Information Architecture for Defense?,” in *New Challenges New Tools for Defense Decisionmaking*. Johnson, Stuart E. and others. Santa Monica CA: RAND, 2003.

-----. *Who Runs What in the Global Information Grid*. Santa Monica CA: RAND, 2000.

Lovelace, Lieutenant General James J. and Brigadier General Joseph L. Votel. "The Asymmetric Warfare Group: Closing the Capability Gaps," *Army Magazine*, 54(3): 29-34 (March 2004).

McKitrick, Jeffrey and others. "The Revolution in Military Affairs," in *Battlefield of the Future: 21st Century Warfare Issues*. Eds. Barry R. Schneider and Lawrence E. Grinter. Studies in National Security No. 3, Air War College (AU), Maxwell AFB AL, September 1998.

Miller, David R. and Michael Gregg. *Security Administrator Street Smarts*. Indianapolis IN: Wiley and Sons Inc, 2008.

President's Information Technology Advisory Committee. *Cyber Security: A Crisis of Prioritization*. Report to the President. Arlington VA: National Coordination Office, 2005.

Ranum, Marcus J. "The Six Dumbest Ideas in Computer Security." 1 September 2005. http://www.ranum.com/security/computer_security/editorials/dumb/

Schneier, Bruce. "Is User Education Working?" April 2006. http://www.schneier.com/essay-139.html

Schneier, Bruce. *Secrets and Lies: Digital Security in a Networked World*. New York: Wiley and Sons Inc, 2000.

Schwartz, General Norton A. "Cyberspace Operations Culture Change." Electronic Message. 10 June 2009.

Seuss, Dr. *Yertle the Turtle and Other Stories*. New York: Random House, 1958.

Smallwood, William L. *Strike Eagle: Flying the F-15E in the Gulf War*. Washington DC: Brassey's Inc, 1998.

US Air Force. *Air Force Doctrine Document 2-4.1 Force Protection*. 9 November 2004.

-----. *Air Force Doctrine Document 3-12 Cyberspace Operations (DRAFT)*. March 2010.

Vest, Hugh S. *Employee Warriors and the Future of the American Fighting Force*. Fairchild Paper. Air University Press, Maxwell AFB AL, 2002.

Wiegmann, Douglas A. and others. *Safety Culture: A Review*. Contract DTFA 01-G-015. Savoy IL: Aviation Research Lab Institute of Aviation, May 2002.

Vita

Major David Perez entered the Air Force through the Reserve Officer Training Corps program at Texas Tech University where he was awarded a B.A. in Communications Studies.

Major Perez is a senior navigator with over 2200 fighter hours. He has accumulated almost 900 combat hours as an F-15E Weapons Systems Officer and EA-6B Electronic Warfare Officer. He was selected to attend AFIT in 2009 and is currently completing Cyber Warfare Intermediate Developmental Education program. Upon graduation, he will be assigned to Combined Air Operations Center Uedem, Germany as a member of the Combat Operations Division conducting Suppression of Enemy Air Defenses/Electronic Warfare planning.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to an penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)* 17-06-2010	**2. REPORT TYPE** Graduate Research Project	**3. DATES COVERED** *(From – To)* 14 May 2009 – 17 Jun 2010

4. TITLE AND SUBTITLE Cyberspace Dependence in Air Force Flying Squadrons and its Effect on Mission Assurance	**5a. CONTRACT NUMBER** N/A **5b. GRANT NUMBER** N/A **5c. PROGRAM ELEMENT NUMBER** N/A
6. AUTHOR(S) David D. Perez, Major, USAF	**5d. PROJECT NUMBER** N/A **5e. TASK NUMBER** N/A **5f. WORK UNIT NUMBER** N/A
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology - Graduate School of Engineering and Management 2950 Hobson Way Wright Patterson Air Force Base, OH 45433-7765	**8. PERFORMING ORGANIZATION REPORT NUMBER** AFIT/ICW/ENG/10-04
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Major Keith Repik (DSN:225-5205, NIPR e-mail: keith.repik@pentagon.af.mil) Chief, Cyber & IO Force Development (AF/A3O-CF) Pentagon, Washington, DC 20330	**10. SPONSOR/MONITOR'S ACRONYM(S)** AF/A30-CF **11. SPONSOR/MONITOR'S REPORT NUMBER(S)** N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

13. SUPPLEMENTARY NOTES
None

14. ABSTRACT

The purpose of this research is to analyze the effects of cyberspace dependence in Air Force flying squadrons. The use of information technology (IT) in the workplace continues to transform the way squadrons conduct operations. While IT enables processes and capabilities, it also adds complexity and vulnerabilities. Therefore, airmen are required to have a higher technical aptitude as well increased awareness of their roles and responsibilities as routine operators of IT systems. This research focuses on exploring these issues and solutions at the squadron level. In order to mitigate dependence on cyberspace at the unit level, the Air Force must address three key issues – squadron culture, squadron organization, and barriers to communication among key actors. Today's Air Force culture fails to stress the importance of computers and networks in daily operations. Current organization in Air Force units provides no central coordination authority for cyber related issues. These problems are just a couple of the reasons that many barriers exist which prevent effective communication between network administrators and end users. Based on an in depth analysis of these issues, this research provides a framework for cultural and organizational change.

15. SUBJECT TERMS
Cyberspace dependence, Mission Assurance, Culture change, Organizational change

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Robert F. Mills, PhD (ENG)
REPORT U	**ABSTRACT** U	**c. THIS PAGE** U	UU	87	**19b. TELEPHONE NUMBER** *(Include area code)* (937)257-3636x4527 robert.mills@afit.edu